高等数学自学丛书

抽象代数

李师正 编

山东教育出版社

责任编辑：徐世典

高等数学自学丛书书目

数学分析基础	线性代数
一元函数微分学	抽象代数
一元函数积分学	空间解析几何
无穷级数	概率论与数理统计
多项式代数	布尔代数

书号 13275·11
定价 1.15 元

高等数学自学丛书

抽象代数

李师正 编

山东教育出版社

一九八三年·济南

内 容 提 要

本书是高等数学自学丛书之一，内容包括集合论基本知识及群胚、半群、群、环、域、代数、模、格等方面的基本概念和性质，并简述伽罗华理论的主要内容。标*号处为选学内容。

本书适合中等学校数学教师、理工科大学生、工程技术人员阅读及青年自学，也可作为高等院校有关专业的教学参考书。

高等数学自学丛书

抽 象 代 数

李 师 正 编

*

山东教育出版社出版

山东省新华书店发行

山东新华印刷厂潍坊厂印刷

*

787×1092 毫米 32 开本　13.75 印张　291 千字

1983 年 4 月新 1 版　1983 年 4 月第 1 次印刷

印数：1—5,500

书号 13275·11　定价 1.15 元

出 版 说 明

为了满足广大读者自学高等数学的需要，我们出版了这套高等数学自学丛书，包括《数学分析基础》、《一元函数微分学》、《一元函数积分学》、《无穷级数》、《多项式代数》、《线性代数》、《抽象代数》、《空间解析几何》、《概率论与数理统计》、《布尔代数》等十册.

这套丛书起点较低，系统性较强，次序的编排尽量作到由浅入深，由易到难，注意循序渐进，并适当渗透了一些现代数学的观点. 在编写过程中，力求作到内容讲述详细，文字通俗顺畅；书中安排了较多的例题和习题，书末附有习题答案或提示. 因此，这套丛书适合自学，也可以作为这些课程的教学参考书.

这套丛书由山东师范大学数学系主持编写. 此外，还得到山东大学数学系、曲阜师范学院数学系、聊城师范学院数学系等单位的大力支持和帮助，在此一并致谢.

一九八二年八月

绪　言

要回答什么是代数，并不是一件容易的事情，因为不同的历史阶段中代数有着不同的含义。

“代数”(Algebra) 一词原由古代一本书的名字(《Al jabr w' al muqâbala》)演化而来，这本书的作者阿里·花拉子米 (Al-Khowârizmî) 是九世纪阿拉伯国家花拉子模的数学家，他在书中记述了解一次及二次方程的法则．不过他所叙述的结果都是用语言而不是用字母表达的，直到十六世纪，法国数学家韦达 (F. Vieta, 1540—1603)首先较系统地创造并利用了字母表示法，后来法国数学家笛卡尔(R. Descartes, 1596—1650) 等人又加以改进，这可以说是数学上的重大变革．至十八世纪，代数被当成用字母表示数构成表达式进行变换和计算的学科．它与算术的区别在于后者总局限于具体数目的运算．从算术到代数，意味着人们思维发展的一次由具体到抽象的飞跃．实际上，当时的代数包揽了除几何外的几乎全部数学．这是代数发展的第一阶段，目前初等代数的内容大体来源于此．

十八世纪末和十九世纪初之后，代数学的中心任务转化为代数方程的求解和研究，代数被认为是有关代数方程理论和方法的学科．与此同时，行列式、矩阵、二次型、线性变换等理论也相应地发展起来．这是代数发展的第二阶段．我们学过的多项式代数和线性代数大都属于这一时期的内容．

自十九世纪后期以来，由于科学的发展，在包括数学本身的许多科学领域中，出现了一些新的量，如向量、矩阵、张量等，它们也有自己的运算，这些运算除适合一些常见的规律外，还有一些特定的规律．如果把这些量用抽象的符号表示，就构成一个个不同的代数系，即带运算的不同集合．撇开具体的量，专门研究抽象代数系的性质，就是代数第三阶段的主要任务．这一阶段常称为抽象代数或近世代数．

实际上，抽象代数的萌芽始于十九世纪之初，因为当时法国青年数学家伽罗华（E. Galois，1811—1832）在彻底解决代数方程能否用根式求解的问题上，曾利用了群论的方法．

整个十九世纪和本世纪二十年代之前，抽象代数处于比较零乱的状态，后来由于一批德国代数学家的综合工作，才统一为一门独立的学科．近几十年来，抽象代数的许多新分支和边缘学科不断涌现，而且在数学和其他科学领域中，如试验设计、计算机科学、图论、几何、分析、理论物理、结构化学等方面应用越来越广泛．总之，抽象代数已成为近代数学中一个十分重要的组成部分．

本书主要讨论抽象代数中的基本代数系——群胚、半群、群、环、域的基本概念和性质，此外还以少量篇幅简单介绍代数、模和格．掌握这些内容不仅是数学工作者以及数学教师所必须的，对于从事其他专业的科学工作者、工程技术人员来说也是很需要的．

在次序的编排上，本书在介绍了必要的预备知识后，先讲述群胚和半群，因为它们不仅是独立的最基本的代数系，而且是群、环、代数等代数系的基础，如群是特殊的半群，

环关于乘法是半群，代数关于乘法是群胚。特别是唯一分解环的非零元作成高斯（Gauss）半群，即唯一分解半群，它的大部分理论只依赖于乘半群的结构，与加法无关。所以，搞清群胚与半群，对后面的学习就会比较顺利，也算本书的一点尝试。伽罗华理论是抽象代数中一颗灿烂的明星，是最著名最精湛的部分之一，但它涉及面广，所以本书仅概述它的主要内容。

目　　录

绪　言

第一章　预备知识 ………………………………………… 1

§1·1　集合及其运算 ………………………………… 1

§1·2　映射 ………………………………………………… 9

§1·3　等价关系与分类 …………………………………20

§1·4　积集与商集 ………………………………………27

§1·5　代数运算 …………………………………………32

本章提要…………………………………………………36

复习题一…………………………………………………37

第二章　群胚与半群 ……………………………………40

§2·1　群胚和半群的概念 ………………………………40

§2·2　半群的整除性 ……………………………………47

§2·3　唯一分解半群 ……………………………………55

§2·4　同态与同构 ………………………………………67

本章提要…………………………………………………73

复习题二…………………………………………………74

第三章　群 ………………………………………………76

§3·1　什么是群?…………………………………………76

§3·2　群的基本性质 ……………………………………81

§3·3　子群 ………………………………………………88

§3·4　陪集 ………………………………………………96

§3·5　循环群……………………………………………101

§3·6　变换群……107
§3·7　置换群……112
§3·8　正规子群与商群……124
§3·9　群的同态……131
§3·10　同构定理……140
§3·11　群的自同态与自同构……146
§3·12　群的直积……152
§3·13　西洛定理……162
*§3·14　可解群与合成群列……170
本章提要……175
复习题三……176
第四章　环……179
§4·1　什么是环？……179
§4·2　环的性质和类型……182
§4·3　子环与理想……191
§4·4　商环与环的同态……196
§4·5　多项式环……209
§4·6　唯一分解环……217
§4·7　素理想与最大理想……227
*§4·8　诺特环中的理想……234
本章提要……240
复习题四……241
第五章　域……244
§5·1　域的基本性质……244
§5·2　分式域……250
§5·3　域的单扩张……257
§5·4　有限扩域与代数扩域……268
§5·5　分裂域……277

§5·6　可分扩域……………………………………………………283
§5·7　有限域……………………………………………………292
*§5·8　伽罗华理论简介…………………………………………298
本章提要 ……………………………………………………306
复习题五 ……………………………………………………307
第六章　代数和模 …………………………………………309
§6·1　代数的基本概念…………………………………………309
§6·2　代数的基本性质…………………………………………314
§6·3　四元数代数………………………………………………323
*§6·4　非结合代数简介…………………………………………328
*§6·5　模…………………………………………………………334
本章提要 ……………………………………………………336
复习题六 ……………………………………………………336
第七章　格 …………………………………………………338
§7·1　半序集……………………………………………………338
§7·2　格的一般概念……………………………………………347
§7·3　分配格与模格……………………………………………355
本章提要 ……………………………………………………362
复习题七 ……………………………………………………362
习题答案与提示 ……………………………………………364
〔附录〕本书符号表 ………………………………………423

第一章 预备知识

这一章是本书的基础，介绍集合、映射、关系、等价关系、分类、积集、商集、代数运算等基本概念.

§1·1 集合及其运算

一、集合与元素

某些确定的对象的集体，称为一个集合. 集合中包含的对象，称为这个集合的元素.

亚洲国家的集合，包括且仅包括地处亚洲的国家.

区间[1,2]中实数的集合，包括且仅包括一切满足 $1\leqslant x\leqslant 2$ 的实数 x.

$M_2(\boldsymbol{R})$——全体实二阶方阵的集合，包括且仅包括一切矩阵$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$，其中$a_{ij}(i,j=1,2)$是任意实数.

集合的例子举不胜举，可以顺手拈来.

集合有一个重要原则，那就是它的元素具有确定性.

给出一个集合，就相当于给出一个明确的判定标准，由它可以判定任意对象在不在这个集合里. 如果没有这样一个标准，或标准不明确，就不算给出一个集合. 如“一切大数的全体”不是一个集合，因为数是不是“大数”，并没有一个明确的标准，比方 10000 算不算大数？10^{10} 算不算大数？

无从得知[注]。

再如分子是偶数的分数的全体，也不是一个集合，因为一个分数属不属于它并不确定。如分数$\frac{1}{2}=\frac{2}{4}$，既不属于它，又属于它。如果说分子是偶数的既约分数（约定分母为正整数）全体就是一个集合了。

集合的元素是确定的，但并不要求元素能一一列举出来。如方程

$$x^5+2x+2=0$$

的复根尽管无法精确地表出（见§5·8 五），但任意复数是不是该方程的根却是完全确定的。事实上，只要代入验证就能判明。所以上述方程的复根组成一个集合。

二、集合描述法

集合常用大写字母 A、B、C、…表示，元素常用小写字母 a、b、c、…或 α、β、…表示。如果 a 是 A 的元素，则记为 $a\in A$，或 $A\ni a$，读作"a 属于 A"或"A 包含 a"。如果 a 不是 A 的元素，则记为 $a\overline{\in} A$ 或 $A\overline{\ni} a$，读作"a 不属于 A"或"A 不包含 a"。

为了表明一个集合含些什么元素，需要对集合进行描述。最常用的是下面两种方法：

1. 列举法：将集合的元素全部开列出来，外加花括号。

如：集合$\{-2, -1, 1, 2\}$，$\{1\}$等，属于用列举法描述集合。有时集合的元素很多，甚至无限多，可以写出少数

注　这种界限不清楚的"集合"，是本世纪六十年代出现的一门新学科——"模糊数学"的研究对象，不属于本书的讨论范围。

元素，以显示出它的规律（如规律不明显，则不能用列举法），后面加上省略号。如

$\{1, 2, 3, 4, \cdots\}$表示自然数集。

$\{1, 3, 5, 7, \cdots\}$表示正奇数集。

$\{2, 4, 6, 8, \cdots, 10000\}$表示2与10000之间的全体偶数组成的集合。

2．叙述法：用集合的元素独具的性质描述集合。

如集合$\boldsymbol{E}=\{$整数$n \mid 2$整除$n\}$表示2的所有倍数组成的集合，即偶数集。$A=\{$实数$x \mid x^2+3x+2=0\}$表示方程$x^2+3x+2=0$的全体实根组成的集合。

叙述法是在花括号中间加一条竖线，左边写元素的一般形式，右边写集合的元素独具的性质。

同一个集合可以用不同的方法描述。如集合$\boldsymbol{E}$和A也可以用列举法写成

$\boldsymbol{E}=\{0, \pm 2, \pm 4, \cdots\}$，$A=\{-1, -2\}$。

三、集合的包含与相等

假设A、B是两个集合，如果集合A的元素都是集合B的元素，则称A属于B，或B包含A，记之$A \subseteq B$，或$B \supseteq A$。这时，也称A是B的子集，B是A的扩集。如$\boldsymbol{E} \subseteq$整数集$\boldsymbol{Z}$。

如果A、B含有完全相同的元素，则称两个集合相等，记之$A=B$。显然，$A=B$的充要条件是$A \subseteq B$且$B \subseteq A$。

如果$A \subseteq B$，但$A \neq B$，则称A是B的真子集，或B真包含A，记之$A \subset B$。这时，B至少有一元素不属于A，但A的元素全部属于B。如$\{2, 4\} \subset \{2, 4, 8\} \subset \boldsymbol{E}$。

四、有限集与无限集

一个集合包含的元素（指不同的元素，下同）可以是任意多个。如集合$\{1\}$，只含一个元素 1，这种只含一个元素的集合称为单元素集。不含任何元素的集合，称为空集合，用ϕ表示。空集可以认为是任何集合的子集。

单元素集与一个元素本身含义不同，而空集也不要与单元素集$\{0\}$相混。

全体实数组成的集合记为$\boldsymbol{R}$，集合

$$\{x\in\boldsymbol{R}\mid(x-1)^2=0\}=\{1\}$$

不能写成 1。集合

$$\{x\in\boldsymbol{R}\mid x^3+x=0\}=\{0\}$$

不是空集ϕ。相反地，集合

$$\{x\in\boldsymbol{R}\mid x^2+2=0\}=\phi$$

（方程$x^2+2=0$无实根）不是$\{0\}$。

集合的元素可以是有限多个，也可以是无限多个，前者称为有限集，后者称为无限集。空集认为是有限集。

有限集S的元素个数是一个非负整数，用记号$|S|$表示。如

$$|\{-1,2,5\}|=3\quad|\{\sqrt{2}\}|=1,$$
$$|\{1,3,5,\cdots,101\}|=51,\ |\phi|=0.$$

如果A是有限集，$B\subseteq A$，则显然B也是有限集，且$|B|\leqslant|A|$；如果$B=A$，则$|B|=|A|$。如果$B\subset A$，则$|B|<|A|$。

五、集合的并集

假定A和B是两个集合，A和B的元素合在一起，又

形成一个新的集合，称为 A 和 B 的并集，记为 $A\cup B$．也就是说，$A\cup B$ 的元素或者属于 A，或者属于 B（包括同时属于 A、B 的元素）（如图1—1）．即

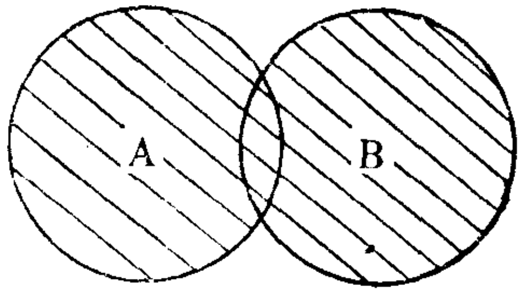


图1—1

$$A\cup B=\{x|x\in A \text{ 或 } x\in B\}.$$

例1　$A=\{1,2,3\}$，$B=\{2,4,6\}$，

则 $A\cup B=\{1,2,3,4,6\}$．

例2　设 $A=\{x\in \mathbf{R}|x>2\}$，

$B=\{x\in \mathbf{R}|x<-1\}$，

则 $A\cup B=\{x\in \mathbf{R}|x>2 \text{ 或 } x<-1\}=\{x\in \mathbf{R}|(x-2)(x+1)>0\}$（如图1—2）．

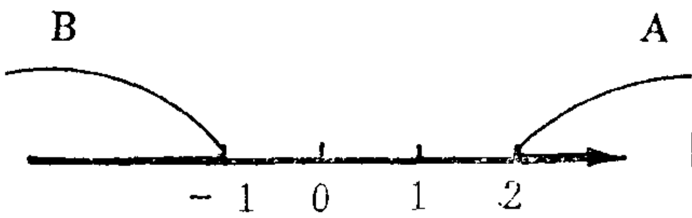


图1—2

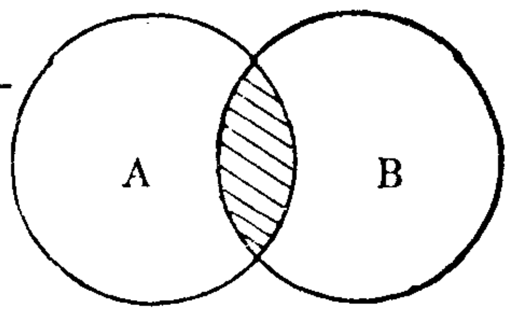


图1—3

六、集合的交集

假定 A 和 B 是两个集合，由同时属于 A 和 B 的元素组成的集合，称为 A 和 B 的交集，记为 $A\cap B$（如图1—3）．即

$$A\cap B=\{x|x\in A \text{ 且 } x\in B\}.$$

例3　设 $A=\{1,2,3\}$，$B=\{2,4,6\}$，

则 $A\cap B=\{2\}$．

例 4 设 $A=\{x\in \mathbf{R} \mid x<2\}$,

$B=\{x\in \mathbf{R} \mid x>-1\}$,

则 $A\cup B=\{x\in \mathbf{R} \mid -1<x<2\}$

$=\{x\in \mathbf{R} \mid (x-2)(x+1)<0\}$ (如图 1—4)．

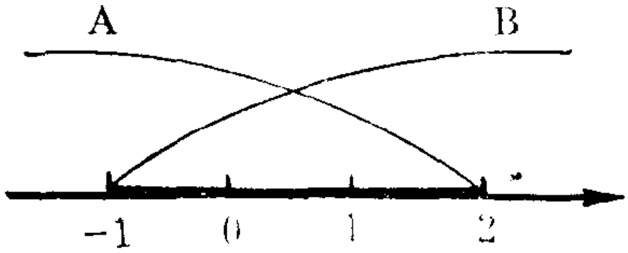


图 1—4

七、并集与交集的性质

定理 1 设 A、B、C 是任意三个集合，则

(1) $A\cup A=A$, $A\cap A=A$(幂等律)；

(2) $A\cup B=B\cup A$, $A\cap B=B\cap A$(交换律)；

(3) $A\cup(B\cup C)=(A\cup B)\cup C$,

$A\cap(B\cap C)=(A\cap B)\cap C$(结合律)；

(4) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$,

$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$(分配律)．

证明：(1)、(2)、(3)是显然的，下面证明(4)的第一式．只须证明左集⊆右集，右集⊆左集．

任取 $x\in$ 左集，则 $x\in A$ 且 $x\in B\cup C$. 如果 $x\in B$，那末 $x\in A\cap B$；如果 $x\in C$，那么 $x\in A\cap C$. 因而 $x\in(A\cap B)\cup(A\cap C)$，即右集．左集⊆右集．

任取 $x\in$ 右集，分两种情况：若 $x\in A\cap B$，那末 $x\in A$ 且 $x\in B$；若 $x\in A\cap C$，那么 $x\in A$ 且 $x\in C$. 不管怎样，总有 $x\in A$，且 $x\in B\cup C$. 因而 $x\in A\cap(B\cup C)$，即右集

$\subseteq$左集，(4)的第一式得证。

(4)的第二式，留作练习。

证毕

多个集合的并集与交集可以类似地定义。如集合 A_1、A_2、…的并集和交集记为 $\bigcup\limits_{n=1}^{\infty} A_n$ 和 $\bigcap\limits_{n=1}^{n} A_n$。

八、集合的差集

假定 A，B 是两个集合。一切属于 A 但不属于 B 的元素组成的集合称为 A 和 B 的差集，记为 $A\setminus B$。即

$$A\setminus B=\{x|x\in A,\ 但\ x\overline{\in} B\}.（如图 1—5）$$

例 5　设 $A=\{1,2,3,4,5\}$，　$B=\{1,3,5,7\}$，则 $A\setminus B=\{2,4\}$。

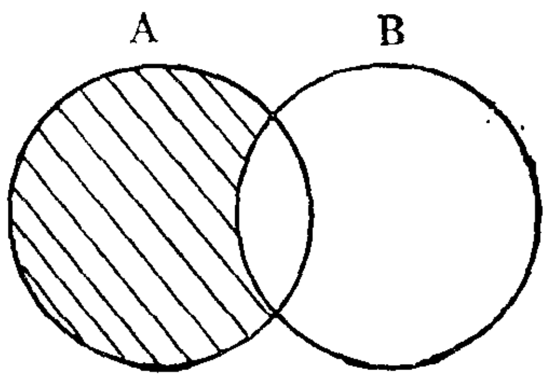


图 1—5

定理 2　设 A，B 是两个集合，则

$$(A\setminus B)\cup B=A\cup B,$$

$$(A\setminus B)\cap B=\phi,$$

$$A=(A\setminus B)\cup(A\cap B).$$

证明留给读者。

习　题　1·1[注]

1．设 $M_1=\boldsymbol{N}$，　$M_2=\boldsymbol{Z}$，　$M_3=\boldsymbol{R}$，　$M_4=\boldsymbol{R}^+$，　$M_5=\{x\in\boldsymbol{R}|x^2=x\}$，$M_6=\{x\in\boldsymbol{R}|x^2\neq x\}$。

(1) 试问下面的数各属于上述的哪些集合？

注　习题中所涉及到的常用数集记号可直接查阅书末附录。

$$0,\ 1,\ \frac{3}{5},\ \sqrt{2},\ -2,\ \pi,\ -\frac{1}{7};$$

（2）写出上述集合的包含关系；

（3）求 $M_1 \cap M_2$，$M_3 \cap M_4$，$M_5 \cup M_6$，$M_4 \cap M_5$，$M_5 \cap M_6$。

2．设$M=\{x \in \mathbf{C} \mid x^5-2x^3+x=0\}$，求$|M|$。

3．设A与B是两个集合，求证：

（1）$A \subseteq A \cup B$，$B \subseteq A \cup B$；

（2）$A \cap B \subseteq A$，$A \cap B \subseteq B$；

（3）如果 $A \cup B=B$，则 $A \subseteq B$；

（4）如果 $A \cap B=A$，则 $A \subseteq B$。

4．设 M为任意集合，求证：

（1）$M \cap \phi=\phi$；

（2）$M \cup \phi=M$。

5．求证：$A=B$ 的充要条件是 $A \cup B \subseteq A \cap B$。

6．证明定理 1 的(4)中第二式，

7．设 A_i 是平面上以原点为心，i 为半径的圆内点集合，试求：

（1）$\bigcup_{i=1}^{\infty} A_i$；　　（2）$\bigcap_{i=1}^{\infty} A_i$。

8．设 A_i 是被 i 整除的自然数集合，即

$$A_i=\{x \in \mathbf{P} \mid i \mid x\},\ i=1,\ 2,\ \cdots.$$

试求：（1）$\bigcup_{i=1}^{\infty} A_i$；（2）$\bigcap_{i=1}^{\infty} A_i$；（3）$A_i \cap A_j$，其中 i，$j \in \mathbf{P}$；（4）$A_i \cup A_j$，其中 i，$j \in \mathbf{P}$。

9．设 A_x 是平面直角坐标系下以$(x,\ 0)$为心，以 1 为

半径的圆周上的点集．试证：$\bigcup_{x \in R} A_x$ 是 x 轴两侧宽为 2 的对称带形区域，其中 R 为实数集．

10．证明定理 2．

11．设 A，B，C 是三个集合，求证：

$$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C).$$

12．设 A 含有 n 个元素，那末 A 的子集共有多少个？为什么？

§1·2 映　　射

这一节讲述映射的概念及其重要特例，如变换、单射、满射、一一映射等．

一、什么是映射？

我们学过函数，任何函数 f 有定义域 A 和值域 B，对于 A 中的每个数 a，由函数法则 f，对应 B 中唯一的数 $b = f(a)$．

函数概念的进一步抽象，就是映射．

定义 1　假设 A、B 是两个集合，如果有一个法则 σ，使 A 中任意元素 a，对应 B 中唯一的元素 $b = \sigma(a)$，则 σ 称为 A 到 B 的映射．b 称为 a 的象，a 称为 b 的一个原象．

也就是说，所谓“A 到 B 的映射”是适合以下三个条件的对应法则：

（1）A 的任意元素都有象；

（2）象全部在 B 中；

（3）A中每个元素的象是唯一的，或者说，A中相同元素的象也相同。

例 1　设$A=\{1,2,3,4\}$，$B=\{1,2,3\}$.规定$\sigma(1)=\sigma(2)=1$，$\sigma(3)=\sigma(4)=2$. σ是A到B的映射(如图 1—6)。

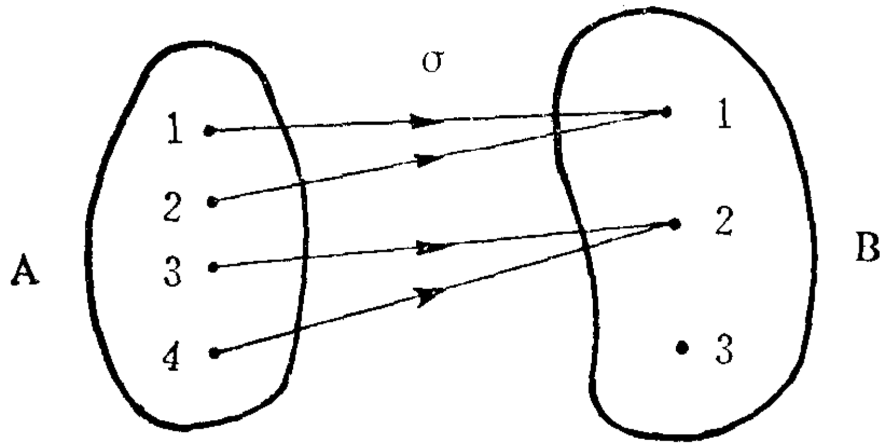


图 1—6

例 2　设$A=B=\boldsymbol{R}[x]$(实数域上的多项式集合)，σ是多项式的求导运算. 因为每个实多项式总有导数，导数是实多项式，并且是唯一的，所以σ是A到B的映射.

例 3　设A是全世界国家的集合，B是全世界城市的集合，规定$\sigma(a)$为国家a的首都. 显然σ是A到B的映射.

例 4　设$A=B=\boldsymbol{R}$(实数集)，规定$\sigma(a)=\lg a$，则σ不是A到B的映射，因为A的元素不全部有象，如-2就没有象. 如果A改为正实数集$\boldsymbol{R}^+$，则σ就是A到B的映射.

例 5　设$A=\boldsymbol{C}$(复数集)，$B=\boldsymbol{R}^*$(非零实数集)，规定$\sigma(a)=|a|$，则σ不是A到B的映射，因为$0+0i$的模是$0\overline{\in}\boldsymbol{R}^*=B$.

例 6　设$A=\{\cos n\pi|n=0,\ \pm 1,\ \pm 2,\ \cdots\}$，$B=\boldsymbol{Z}$(整数集)，$\sigma(\cos n\pi)=n$，则$\sigma$不是$A$到$B$的映射，因为按

照映射的唯一性要求，相同元素的象也应相同，然而 $\cos\pi = \cos 3\pi = -1$，却有 $\sigma(\cos\pi)=1$，$\sigma(\cos 3\pi)=3$。实际上，A 只含两个元素：1 和 -1，但 -1 至少有两个象 1 和 3。

注意：映射只要求每个元素的象唯一，并不要求原象唯一，如例 1 中 1 的原象有两个：1 和 2。另一方面，A 到 B 的映射并不要求 B 的每个元素有原象。如例 1 中 B 的元素 3 就无原象。

二、象集与原象集

设 σ 是 A 到 B 的映射，A_1 是 A 的子集，那么 σ 也是 A_1 到 B 的映射，A_1 中所有元素的象构成 B 的一个子集，记为 $\sigma[A_1]$，即

$$\sigma[A_1]=\{\sigma(a)\mid a\in A_1\},$$

称为 A_1 的象集（如图 1—7）。

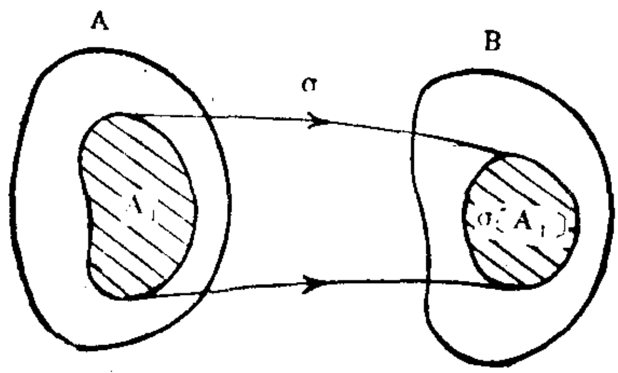


图 1—7

另一方面，设 B_1 是 B 的子集、B_1 的元素的所有原象又构成 A 的子集，称为 B_1 的原象集，记为 $\sigma^{-1}[B_1]$，即

$$\sigma^{-1}[B_1]=\{a\in A\mid \sigma(a)\in B_1\}$$

原象集可以是空集（如图 1—8）。

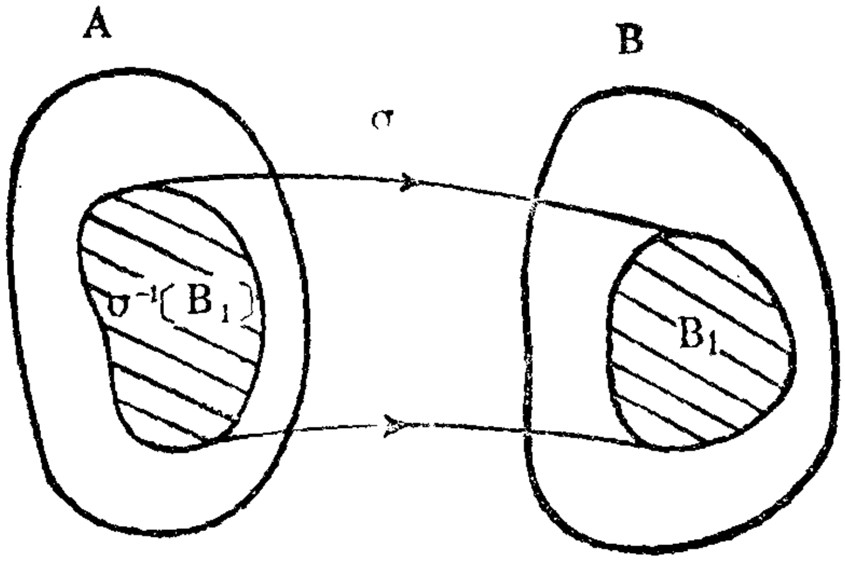


图 1—8

例 7 复数集 $\boldsymbol{C}$ 到实数集 $\boldsymbol{R}$ 的映射 σ 规定为 $\sigma(r)=|r|$. 整数集 $\boldsymbol{Z}$ 是 $\boldsymbol{C}$ 的子集，其象集为非负整数集 $\boldsymbol{N}$，即

$$\sigma[\boldsymbol{Z}]=\boldsymbol{N}.$$

区间 $[0,1]$ 是 $\boldsymbol{R}$ 的子集，其原象集是全体模不大于 1 的复数组成的集合.

区间 $(-2,-1)$ 也是 $\boldsymbol{R}$ 的子集，但它的原象集是空集，因为没有模小于零的复数.

注意 A 到 B 的映射下，A 子集 A_1 的象集的原象集总包含 A_1，一般不等于 A_1. 如上例中，集合 $A_1=\{bi|b\in\boldsymbol{R}\}$ 的象集是 $\boldsymbol{R}^+\cup\{0\}$（即全体非负实数的集合），但 $\boldsymbol{R}^+\cup\{0\}$ 的原象集是 $\boldsymbol{C}$，$A_1\subset\boldsymbol{C}$.（$\boldsymbol{R}^+$ 是正实数集）

三、映射的相等

定义 2 设 σ 和 τ 都是集合 A 到集合 B 的映射，如果对于 A 中的每个元素 a，都有 $\sigma(a)=\tau(a)$，则称映射 σ 和 τ 相等，记为 $\sigma=\tau$.

例 8 设 $A=B=\{1, 2, 3\}$，对于任意的 $a\in A$，规定 $\sigma(a)=\cos 2a\pi$，$\tau(a)=1$。

由于 $\sigma(1)=\tau(1)=1$，$\sigma(2)=\tau(2)=1$，$\sigma(3)=\tau(3)=1$，故 $\sigma=\tau$。

映射的相等显然与所考虑的集合有直接关系，上例如果把 A 和 B 改为实数集，那末 σ 和 τ 就不相等，因为例如 $\sigma\left(\frac{1}{2}\right)=\cos\pi=-1$，而 $\tau\left(\frac{1}{2}\right)=1$。

四、变换

定义 3 非空集合到自身的映射，称为这个集合的变换。

最简单的变换是恒等变换，它是使集合中所有元素不变的变换。集合 A 的恒等变换记为 ε_A。

设 σ 和 τ 是集合 A 的变换，对于任意的 $a\in A$，规定

$$\tau\sigma(a)=\tau(\sigma(a)),$$

这样形成的 A 的变换 $\tau\sigma$，称为 τ 与 σ 的乘积。它是先施行变换 σ，再施行变换 τ 的合成变换(如图 1—9)。

注意：变换次序是自右而左。

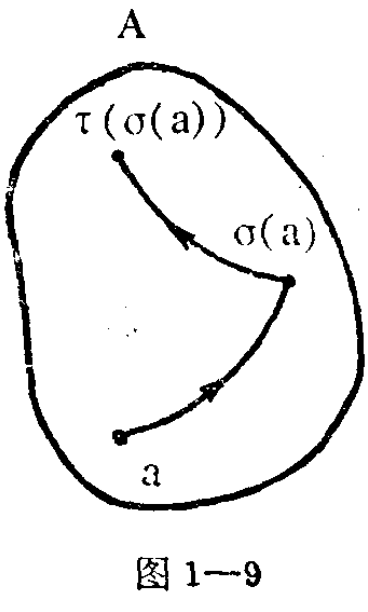


图 1—9

例 9 设 A 是平面上点的集合，σ 为绕原点 O 旋转 $90°$ 的变换，τ 为沿 y 轴正向平移 1 的变换，则 $\tau\sigma$ 是先旋转 $90°$ 角后沿 y 轴平移 1 的合成变换。

变换的乘积一般是不可换的，如在上例中，$\sigma\tau$ 是沿 y 轴正

向平移 1 再旋转 90° 的变换，两种合成变换是不同的，例如点(1,0)，经 $\tau\sigma$ 变为 (0,2)，而经 $\sigma\tau$ 则变为 (-1,1)，故有 $\tau\sigma\neq\sigma\tau$.（如图 1—10）

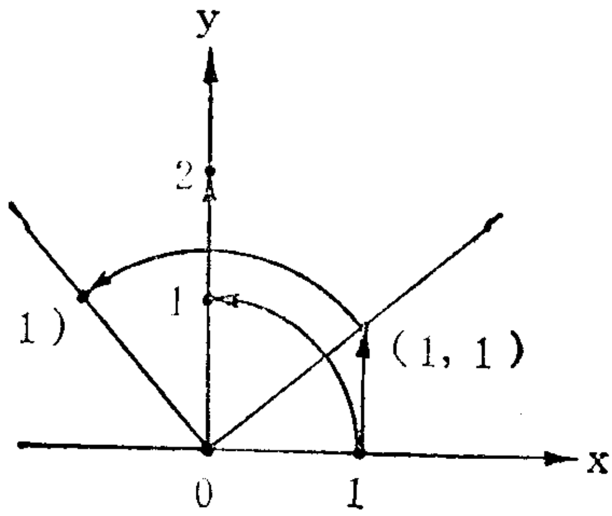


图 1—10

变换的乘法虽然不适合交换律，但适合结合律。

定理 1 设 σ_1，σ_2，σ_3 是集合 A 的变换，则有

$$(\sigma_3\sigma_2)\sigma_1=\sigma_3(\sigma_2\sigma_1). \tag{1}$$

分析：证明对所有 $a\in A$，经(1)式两端的变换的象相同。

证明：任取 $a\in A$，则有

$$((\sigma_3\sigma_2)\sigma_1)(a)=(\sigma_3\sigma_2)(\sigma_1(a))=\sigma_3(\sigma_2(\sigma_1(a))).$$

$$(\sigma_3(\sigma_2\sigma_1))(a)=\sigma_3((\sigma_2\sigma_1)(a))=\sigma_3(\sigma_2(\sigma_1(a))).$$

所以(1)式成立。

证毕

五、单射、满射与一一映射

集合 A 到集合 B 的映射使 A 的每个元素有唯一的象，但不同的元素可能有相同的象，如例 2 中 $x+2$ 与 $x+1$ 有相同的象，因为它们的导数都是 1．如果一个映射使不同元素的

象也不同，则称之为单射.

例 3 的映射是单射，因为不同国家的首都也不相同.

集合 A 到集合 B 的映射 φ 下象集 $\varphi[A]$ 是 B 的子集. 如果 $\varphi[A]=B$，则称 φ 是 A 到 B 的满射. 这时，象集充满了集合 B，即 B 的每个元素都是 A 的某元素的象.

例 1 和例 3 中的映射显然不是满射，而例 2 中的映射是满射，因为每个多项式的不定积分都是多项式，而后者的导数正是原多项式.

显然，当且仅当对每个 $b\in B$，$\varphi^{-1}[b]\neq\phi$ 时，φ是满射；当且仅当对每个 $b\in\varphi[A]$，$\varphi^{-1}[b]$是单元素集时，φ 是单射.

满射与单射之间并没有必然的联系. 满射可以是单射，也可以不是.

既是满射又是单射的映射，称为一一映射. 集合 A 与集合 B 之间如果存在一一映射，则称 A 与 B 有一一对应.

如 A 是某班学生的集合，B 是学生座号的集合，φ 是学生到座号的对应法则，则 σ 是 A 到 B 的一一映射，A 与 B 有一一对应.

集合 A 到 A 的满射、单射和一一映射，分别称为 A 的满射变换、单射变换和一一变换.

六、逆映射

如果 σ 是集合 A 到集合 B 的一一映射，则对于每个 $b\in B$，有唯一的原象 a. 这样，又确定了一个由 B 到 A 的对应法则，而且是映射. 这个由 σ 决定的 B 到 A 的映射，称为 σ 的逆映射，记为 σ^{-1}. 当 $A=B$ 时，逆映射称为逆变换.

一一映射是满射，所以 A 到 B 的一一映射 σ 使 B 的每个

元素是A的某一元素的象，而一一映射又是单射，因而B的每个元素的逆象是唯一的．这样，σ的逆映射必是B到A的一一映射．

例 10 考虑由实数集$\boldsymbol{R}$到正实数集$\boldsymbol{R}^+$的映射σ：$\sigma(x)=10^x$，$x\in\boldsymbol{R}$．显然σ是满射．此外，如果$x_1\neq x_2$，则$10^{x_1}\neq 10^{x_2}$，因而σ是单射，从而σ是一一映射．易见，$\sigma^{-1}(y)=\lg y$，σ^{-1}是$\boldsymbol{R}^+$到$\boldsymbol{R}$的一一映射．

从函数观点来看，$\lg y$正是10^x的反函数，所以，可以认为逆映射是反函数概念的推广．

定理 2 如果σ是集合A的一一变换，则$\sigma^{-1}\sigma=\sigma\sigma^{-1}$是$A$的恒等变换$\varepsilon_A$．

分析：只须证明对于任意$a\in A$，$(\sigma^{-1}\sigma)(a)=(\sigma\sigma^{-1})(a)=a$．

证明：任取$a\in A$，设$\sigma(a)=b$，则$\sigma^{-1}(b)=a$．因而$\sigma^{-1}(\sigma(a))=\sigma^{-1}(b)=a$．或者说，

$$(\sigma^{-1}\sigma)(a)=a.$$

设$\sigma(c)=a$，即$\sigma^{-1}(a)=c$，$\sigma(\sigma^{-1}(a))=\sigma(c)=a$．或者说，

$$(\sigma\sigma^{-1})(a)=a.$$

因而，$\sigma^{-1}\sigma=\sigma\sigma^{-1}=\varepsilon_A$．

证毕

定理 2 的逆命题也成立．

定理 3 设σ和τ是集合A的变换，如果$\sigma\tau=\tau\sigma=\varepsilon_A$，那末$\sigma$和$\tau$都是$A$的一一变换，且$\tau=\sigma^{-1}$，$\sigma=\tau^{-1}$．

分析：先证σ和τ是满射变换，且是单射变换，最后证明τ和σ互为逆变换．

证明：(1) 任取 $a\in A$．由于 $\sigma\tau$ 是恒等变换，所以

$$\sigma(\tau(a))=(\sigma\tau)(a)=a.$$

设 $\tau(a)=b$，即 $\sigma(b)=a$，因而 $a\in\sigma[A]$，$A\subseteq\sigma[A]$．而显然 $\sigma[A]$是A的子集，所以 $\sigma[A]=A$，σ 是满射变换．同理，τ 也是满射变换．

(2) 如果 a_1，$a_2\in A$，$\sigma(a_1)=\sigma(a_2)$．由于 $\tau\sigma$ 是恒等变换，因而

$$a_1=\tau\sigma(a_1)=\tau(\sigma(a_1)),$$

$$a_2=\tau\sigma(a_2)=\tau(\sigma(a_2)).$$

上面两式右端相等，所以 $a_1=a_2$，即 σ 是单射变换．同理 τ 是单射变换．

因而，σ 和 τ 都是一一变换．

(3) 设 σ 的逆变换为 σ^{-1}，任取 $a\in A$，则 $\sigma\tau(a)=a$，$\sigma^{-1}(a)=\sigma^{-1}(\sigma\tau(a))=(\sigma^{-1}\sigma)(\tau(a))=\tau(a)$．所以 $\sigma^{-1}=\tau$．同理 $\tau^{-1}=\sigma$．

证毕

综合定理 2 和定理 3，可得

推论 1 集合A的变换 σ 为一一变换的充要条件是存在变换 τ，使 $\sigma\tau=\tau\sigma=\varepsilon_A$．

关于集合的变换和一一变换，在第三章还要详细讨论．

七、集合的等势

定义 4 设A和B是两个非空集合．如果A和B有一一对应，则称A和B等势，记为$A\sim B$．否则，记为$A\not\sim B$．此外，认为空集与本身等势．

定理 4 有限集A和B等势的充要条件是$|A|=|B|$．

证明：如果 $A\sim B$，设 $A=\{a_1, a_2,\cdots,a_n\}$，$\sigma$ 是 A 到 B 的一一映射，$b_i=\sigma(a_i)$，$i=1,2,\cdots,n$，则 b_i 两两不同，且 $B=\{b_1, b_2\cdots, b_n\}$。因而 $|A|=|B|=n$。

反之，如果 $|A|=|B|=n$，设 $A=\{a_1, a_2, \cdots ,a_n\}$，$B=\{b_1, b_2\cdots, b_n\}$，规定 A 到 B 的映射 σ 为 $\sigma(a_i)=b_i$，$i=1,2,\cdots,n$，则 σ 显然是 A 到 B 的一一映射，因而 $A\sim B$。

证毕

推论 2 有限集不与其真子集等势。

证明：设 B 为有限集 A 的真子集，则 $|B|<|A|$。如果 $A\sim B$，由以上定理，$|A|=|B|$，推出矛盾。

证毕

注意：无限集可与真子集等势。如 $\sigma(n)=2n$ 是整数集 $\mathbf{Z}$ 到偶数集 $\mathbf{E}$ 的一一映射，所以 $\mathbf{Z}\sim\mathbf{E}$，而 $\mathbf{E}$ 是 $\mathbf{Z}$ 的真子集。再如 $\sigma(x)=\frac{2}{\pi}\operatorname{arc\,tg} x$ 是 $\mathbf{R}$ 到开区间 $(-1,1)$ 的一一映射，因而 $\mathbf{R}\sim(-1,1)\subset\mathbf{R}$。

等势具有反身性、对称性和传递性，即有

定理 5 (1) 集合 A 与自身等势，即 $A\sim A$。

(2) 如果集合 A 与集合 B 等势，则集合 B 与集合 A 等势。

(3) 如果集合 A 与集合 B 等势，集合 B 与集合 C 等势，则集合 A 与集合 C 等势。

证明留给读者。

习 题 1·2

1. 下列对应法则哪些是 R 的变换?哪些是满射变换?单射变换?一一变换?

(1) $\sigma(a)=a-1$;　　(2) $\sigma(a)=a^2$;

(3) $\sigma(a)=\frac{a+1}{a-1}$;　　(4) $\sigma(a)=\lg(a+1)$;

(5) $\sigma(a)=\sqrt{a+1}$;　　(6) $\sigma(a)=a^3$;

(7) $\sigma(a)=\begin{cases}a+1,(a\geqslant 0);\\ a,(a<0).\end{cases}$　　(8) $\sigma(a)=\begin{cases}a-1,(a\geqslant 0);\\ a,(a<0).\end{cases}$

2. 集合 A 的变换 σ 的不动元是指这样的元素 a: $\sigma(a)=a$. 试判断上题各变换是否有不动元?

3. 设 $A=\{1,2,3,4\}$, σ 和 τ 是 A 的变换, 且已知: $\sigma(1)=\sigma(2)=1$, $\sigma(3)=2$, $\sigma(4)=3$; $\tau(1)=2$, $\tau(2)=3$, $\tau(3)=4$, $\tau(4)=1$. 试写出 $\sigma\tau$ 和 $\tau\sigma$ 对于 A 中每个元素的象.

4. 如果 σ 是集合 A 的一一变换, 求证: $(\sigma^{-1})^{-1}=\sigma$.

5. 如果 σ 和 τ 都是集合 A 的一一变换, 求证: $\sigma\tau$ 也是 A 的一一变换, 且 $(\sigma\tau)^{-1}=\tau^{-1}\sigma^{-1}$.

6. 如果 A 是有限集, $B\subseteq A$, 且 $B\sim A$, 求证: $B=A$.

7. 证明: $\mathbf{N}\sim\mathbf{Z}$.

8. 设 A、B 是有限集. 如果存在 A 到 B 的满射, 则 $|B|\leqslant|A|$; 如果存在 A 到 B 的单射, 则 $|B|\geqslant|A|$.

9. 设 A、B 为有限集, $A\sim B$, 则 A 到 B 的满射或单射也是一一映射. 上述性质对无限集是否成立? 试举一例.

10. 证明定理 5.

§1·3 等价关系与分类

本节讨论集合中的关系、等价关系与分类，并证明等价关系与分类的一致性。

一、关系

在实数集 $\boldsymbol{R}$ 中，任意两个数 a 与 b 之间，要么 $a<b$，要么 $a \nless b$。如果 $a<b$，则称 a 和 b 有“$<$”关系；如果 $a \nless b$，则称 a 和 b 无“$<$”关系。

在实多项式集 $\boldsymbol{R}[x]$ 中，对于任意两个多项式 $f(x)$ 和 $g(x)$，$f(x)|g(x)$ 或 $f(x)\nmid g(x)$ 有且仅有一种关系成立，如果 $f(x)|g(x)$，称 $f(x)$ 和 $g(x)$ 有整除关系，否则称 $f(x)$ 和 $g(x)$ 无整除关系。

下面引进任意集合中“关系”的概念。把上述 $<$ 及 $|$ 抽象为符号 R，于是有

定义 1 设 A 是非空集合，R 是 A 中的一个法则，如果对于任何一对有序元素 a、b，要么 aRb 成立，要么 aRb 不成立，则称 R 是 A 的一个关系。这时，如果 aRb 成立，则称 a 和 b 有关系 R，否则称 a 和 b 无关系 R，后者记为 $a\bar{R}b$。

上面提到的 $\boldsymbol{R}$ 中的“$<$”和 $\boldsymbol{R}[x]$ 中的“整除”都是关系。

例 1 设 A 是任意非空集合，记 $F(A)$ 为 A 的所有子集构成的集合族。集合的包含($\subseteq$)是 $F(A)$ 的一个关系，这是因为对于任意 S、$T\in F(A)$，$S\subseteq T$ 或 $S\nsubseteq T$ 有且仅有一种成立。

例 2 设 A 是某栋宿舍楼中全体居民的集合，对于 a, $b\in A$，约定 aRb 当且仅当 a 是 b 的后代。因为对于 A 中任意两个人 a 和 b，a 是否 b 的后代是唯一确定的，所以 R 是 A 的一个关系。

例 3 复数集 C 中规定 aRb 当且仅当 $|a|=|b|$。R 是 C 的一个关系，因 a 和 b 的模是否相等是唯一确定的。

例 4 有理数集 Q 中规定 $\frac{b}{a}R\frac{d}{c}$ 当且仅当 $b>d$ 时，则 R 不是 Q 的关系，因为两个有理数是否有上述关系 R 不是唯一确定的。如 $\frac{2}{3}$ 和 $\frac{1}{2}$，一方面，因 $2>1$，所以 $\frac{2}{3}R\frac{1}{2}$；另一方面，$\frac{1}{2}=\frac{3}{6}$，所以 $\frac{2}{3}\bar{R}\frac{3}{6}$。

例 5 正整数集 P 中规定 aR_1b 当且仅当 $a+b<0$。而 P 中任意两个元素之和都大于零，R_1 是 P 的一个关系，但是 P 的任意两个元素都无关系 R_1。这样的关系称为空关系。

P 中若规定 aR_2b 当且仅当 $a+b>0$，则显然 P 中任意两个元素都适合这一不等式，因而 R_2 是 P 的一个关系，且 P 中任意两个元素都有关系 R_2。这样的关系称为全关系。

二、等价关系

在例 3 中，关系 R 显然有以下三个性质：

(1) 对每个 a，都有 aRa；(反身性)

(2) 如果 aRb，则 bRa；(对称性)

(3) 如果 aRb，bRc，则 aRc。(传递性)

具有以上性质的关系特别重要。

定义 2 设 E 是集合 A 的一个关系，如果具有反身性、对

称性和传递性，则 E 称为 A 的一个等价关系。这时，如果 aEb，则称 a 等价于 b，记为 $a\overset{E}{\sim}b$，或 $a\sim b(E)$，或 $a\sim b$。

例 1 中的关系 R 具有反身性和传递性，但不具有对称性；例 2 中的关系具有传递性，但不具有反身性和对称性，所以都不是等价关系。

例 6　设 A 是任意非空集合，规定 aEb 当且仅当 $a=b$，E 是等价关系。

事实上，a 是否等于 b 是完全确定的，所以 E 是 A 的一个关系。E 的反身性、对称性和传递性是显然的。

例 7　已知 n 是一个固定正整数，整数集 $\mathbf{Z}$ 中规定 aEb 当且仅当 $n\mid a-b$（即 a 和 b 用 n 除的余数相同，这时称 a 与 b 关于 n 同余，常记为 $a\equiv b(\bmod n)$），E 是等价关系。

事实上，对于任意 a、$b\in\mathbf{Z}$，$a-b$ 能否被 n 整除是唯一确定的，所以 E 是关系。下面证明 E 是等价关系。

对每个 $a\in\mathbf{Z}$，显然 $n\mid a-a$，故 aEa，反身性成立；

如果 aEb，则 $n\mid a-b$，$n\mid b-a$，因而 bEa，对称性成立；

如果 aEb，bEc，则 $n\mid a-b$，$n\mid b-c$，因而 $n\mid a-c$，即 aEc，传递性成立。

例 8　实数集 $\mathbf{R}$ 中规定 aRb 当且仅当 $a^2+b^2=0$。R 是关系，但不是等价关系，因为 R 尽管有对称性和传递性，却没有反身性，如 $1^2+1^2=1\neq0$，故 $1\bar{R}1$。

例 9　$\mathbf{R}$ 中通常的“$\geqslant$”不是等价关系，这是因为它尽管有反身性和传递性，但没有对称性，如 $3\geqslant2$，却 $2\ngeqslant3$。

例 10　$\mathbf{R}$ 中规定 aRb 当且仅当 $|a-b|\leqslant1$。R 不是等价关系，这是因为 R 尽管有反身性和对称性，但没有传递性，如

$0R\frac{2}{3}$，$\frac{2}{3}R\frac{4}{3}$，却 $0\bar{R}\frac{4}{3}$.

例 8～10 中，每个关系都仅违背了等价关系三原则之一，说明这三个原则是互相独立的，不能互相推证。有人将反身性当成对称性与传递性的推论，理由是：

由 aRb 得 bRa，又由 aRb，bRa，得 aRa。因而得反身性。

这里无形中作了如下假定：

(1′) 对每个 a，存在 b，使 aRb。

刚才的推理说明由(1′)和对称性、传递性可推出反身性。但如果没有(1′)，仅由对称性、传递性是得不出反身性的，例 8 就说明这一点。另外，由反身性显然可以推出(1′)(取 $b=a$)，所以，(1′)可以用来代替等价关系定义中的反身性。

三、分类

我们常根据某种需要，把一个集合分成若干子集，使每个元素属于且仅属于其中一个子集。如全国分成若干省(市)、自治区，一个学校分成若干班，整数分为奇数与偶数等。

定义 3 非空集合 A 如果表为若干两两不相交的非空子集的并[注]，则称这些子集为集合 A 的一种分类。其中每个子集，称为一个类。

换句话说，A 的子集族 $\{A_\lambda\}$ 形成 A 的一种分类，是指：

(1) $\bigcup A_\lambda = A$；

(2) 当 $\lambda \neq \mu$ 时，$A_\lambda \cap A_\mu = \phi$。

其中第 1 说明这些 A_λ 无遗漏地包含了 A 的全部元素，第

注 两两不相交，指任何两个子集的交都是空集。

2 说明两个不同的 A_λ 无公共元素，即 A 的每个元素属于且仅属于一个子集 A_λ. 它们常称为分类的不漏不重原则(如图 1—11).

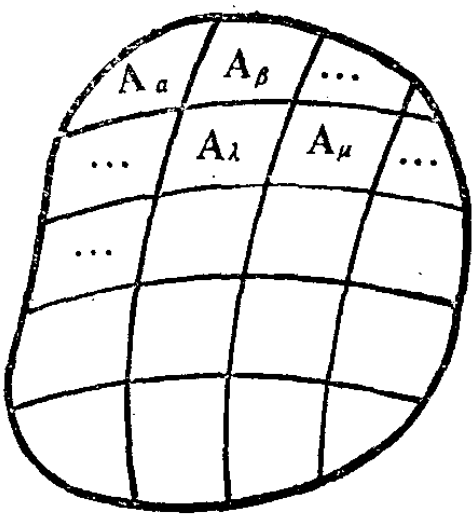


图 1—11

例 11　实多项式集 $\boldsymbol{R}[x]$ 中，用 A_{-1} 记零多项式构成的单元素集，A_0 记零次多项式（非零实数）集，A_1 记一次多项式集，A_2 记二次多项式集，…，则 $\{A_i \mid i=-1,0,1,2,\cdots\}$ 是 $\boldsymbol{R}[x]$ 的一种分类，因为任意实多项式属于且仅属于其中某一 A_i.

例 12　复数集 $\boldsymbol{C}$ 中定义 $A_\lambda=\{z\in\boldsymbol{C}\mid |z|=\lambda\}$，$\lambda\in\boldsymbol{\Lambda}$，$\boldsymbol{\Lambda}$ 是全部非负实数形成的集合. 每个复数有唯一的模，它是一个非负实数，所以 $\{A_\lambda \mid \lambda\in\boldsymbol{\Lambda}\}$ 是 $\boldsymbol{C}$ 的一种分类.

例 13　实数集 $\boldsymbol{R}$ 中定义 $A_i=(i-1,\ i)$，$i\in\boldsymbol{Z}$，则 $\{A_i \mid i\in\boldsymbol{Z}\}$ 不是 $\boldsymbol{R}$ 的分类，因为每个整数不在任何一个 A_i 中.

例 14　$\boldsymbol{R}$ 中定义 $A_i=[i-1,i+1]$，$i\in\boldsymbol{Z}$，则 $\{A_i \mid i\in\boldsymbol{Z}\}$ 也不是 $\boldsymbol{R}$ 的分类，因为整数 i 既在 A_i 又在 A_{i+1} 中.

注意：集合 A 的分类，对类的个数并无附加要求，既使整个 A 当成一类，或每个元素独占一类也无不可，前者是最“粗”的分类；后者是最“细”的分类.

分类中每类所含元素的个数不一定相同，如例 11 中，$|A_{-1}|=1$，而其他各类都是无限集.

四、等价关系与分类

集合中元素的等价关系与元素的分类实质上是一致的.

首先，如果集合A里面有一个等价关系，那末对于任意$a\in A$可以建立一个集合$[a]$，它由一切与a等价的元素组成：

$$[a]=\{x\in A\mid x\sim a\}.$$

$[a]$称为包含a的等价类．下面我们证明全体这样的等价类形成A的一种分类．

事实上，A的任意元素a显然属于类$[a]$．而如果两个类$[a]$和$[b]$有共同元素c的话，则$c\sim a$，$c\sim b$，推出$a\sim b$，$a\in[b]$；同理又有$b\in[a]$，因而$[a]\subseteq[b]$，$[b]\subseteq[a]$，$[a]=[b]$．也就是说，两个不同的等价类不会有任意共同元素．从而全体等价类形成A的分类．

反之，如果已知集合A的一种分类，在A中，规定aEb当且仅当a与b在同一类里，则E是A的等价关系．

事实上，E显然是A的关系．此外：

(1) 对每个$a\in A$，a与本身同类，故总有aEa；

(2) 如有aEb，说明a与b同类，当然b与a同类，故bEa；

(3) 如有aEb，bEc，说明a与b同类，b与c同类，因而a与c同类，即aEc．

等价关系E下的等价类与原有的分类显然是一致的．

例3的等价关系与例12的分类是相互对应的；例11的分类决定的等价关系是$f(x)\sim g(x)$当且仅当$f(x)$与$g(x)$同次数(约定零多项式只与自身同次数)；例6的等价关系决定的分类是最细的分类，每类只含一个元素．

五、整数的剩余类

例7建立了$\mathbf{Z}$中的一个等价关系，因而也形成了$\mathbf{Z}$的

一种分类，称为以 n 为模的剩余类：

$[0]=\{\cdots,\ -2n,\ -n,\ 0,\ n,\ 2n,\ \cdots\}$,

$[1]=\{\cdots,\ -2n+1,\ -n+1,\ 1,\ n+1,\ 2n+1,\ \cdots\}$,

……………………………………………………………………

$[n-1]=\{\cdots,\ -n-1,\ -1,\ n-1,\ 2n-1, 3n-1, \cdots\}$.

记 $\mathbf{Z}_n=\{[0],\ [1],\ \cdots,\ [n-1]\}$，其元素是剩余类，而非整数。每个剩余类中，任意两整数相差 n 的整数倍。

例 15 $\mathbf{Z}_3=\{[0],\ [1], [2]\}$. 图 1—12 内 [0] 中数标以·，[1]中数标以▲，[2] 中数标以×.

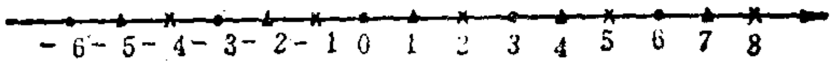


图 1—12

习 题 1·3

1．复数集 C 的下列关系是否等价关系？

(1) z_1Rz_2 当且仅当 $|z_1|\geq|z_2|$；

(2) z_1Rz_2 当且仅当 $z_1=z_2+i$；

(3) z_1Rz_2 当且仅当 $z_1/z_2=1$；

(4) z_1Rz_2 当且仅当 $\mathrm{Re}\, z_1=\mathrm{Re}\, z_2$；

(Re z 表示 z 的实部)

(5) z_1Rz_2 当且仅当 $z_1^2=z_2^2$；

(6) z_1Rz_2 当且仅当 $z_1\neq z_2$；

(7) z_1Rz_2 当且仅当 $z_1\neq 0$；

(8) z_1Rz_2 当且仅当 $z_1=-z_2$；

(9) z_1Rz_2 当且仅当 $z_1=Z_2$；

(10) $z_1 R z_2$ 当且仅当 $\frac{1}{z_0}(z_1 - z_2)$ 是实数，其中 $z_0 \neq 0$ 是固定复数。

2. 上题中的等价关系所对应的等价类为何？

3. 设 σ 是 A 到 B 的映射，在 A 中规定：aEb 当且仅当 $\sigma(a)=\sigma(b)$.求证：E是A 的等价关系.其等价类是什么？

*4. 四个元素构成的集合里，有几种不同的分类？

5. $\sigma(z)=|z|$ 是 $\boldsymbol{C}^*$到 $\boldsymbol{R}$ 的映射. 试问，由 σ 决定的 $\boldsymbol{C}^*$ 的等价类是什么？（见本习题第 3 题）

6. 在实 n 阶方阵集 $M_n(\boldsymbol{R})$中，规定：

(1) $A \sim B$ 当且仅当存在非退化方阵 T，使 $B=TAT^{-1}$，求证$\sim$是等价关系；

(2) $A \approx B$ 当且仅当存在非退化方阵 P，使 $B=PAP'$，求证$\approx$是等价关系.

*7. 设 ρ 和 σ 是集合 A 的两个关系，在 A 中规定：$a\tau b$ 当且仅当存在 $c\in A$，使 $a\rho c$，$c\tau b$，求证 τ 是 A 的关系. 当 ρ 和 σ 是等价关系时，τ 是否等价关系？

§1·4 积集与商集

由已知集合也可以产生出新的集合来，本节将介绍两种途径，即积集与商集.

一、积集

设 $A=[0,2]$，$B=[-1,0]$是两个实数区间，从 A 中任取一个数 x，B 中任取一个数 y，组成一个有次序的数对

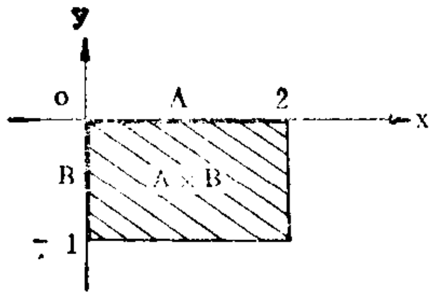


图 1—13

(x,y).这个数对里永远保持第一个数在 A 中，第二个数在 B 中．现在让 x 跑遍 A，y 跑遍 B，得到的所有数对组成一个新的集合，叫做积集 $A\times B$（如图 1—13）．

一般地，我们有

定义 1 设 A、B 是两个非空集合．形如 (a,b) 的有序对的全体组成的集合，其中 $a\in A, b\in B$，称为 A 与 B 的积集，记为 $A\times B$．即

$$A\times B=\{(a,b)\mid a\in A, b\in B\}.$$

除 $A=B$ 外，$A\times B$ 和 $B\times A$ 是两个不同的集合．如刚才的例子中，$B\times A$ 如图 1—14 所示，与 $A\times B$ 显然不同．

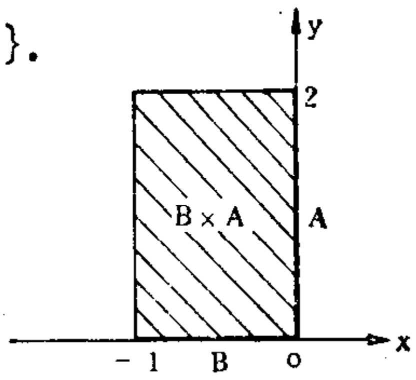


图 1—14

积集的元素 $(a,b)=(a_1,b_1)$ 是指 $a=a_1$ 且 $b=b_1$．

例 1 设 $A=\{1,2,3\}$，$B=\{1,2\}$，则

$A\times B=\{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2)\}$.

例 2 $R\times R$ 是一切有序实数对 (x,y) 的集合，它也可以看作平面上所有点组成的集合．注

二、积集与关系

设集合 $A\neq\phi$，S 是积集 $A\times A$ 的子集．在 A 中规定：

注 $R\times R$ 以后常记为 R_2．

aRb 当且仅当$(a,b)\in S$。由于对于任意 a、$b\in A$，$A\times A$ 的元素(a,b)属不属于 S 是唯一确定的，所以 aRb 或 $a\bar{R}b$ 有且仅有一个成立，即 R 是 A 的关系。就是说，由 $A\times A$ 的任一集合，可以形成 A 的一个关系。

反之，如果 A 中有某一关系 R，我们构造集合

$$S_R=\{(a,b)\in A\times A \mid aRb\},$$

S_R 由一切有关系 R 的元素对 (a,b)组成。

总之，给出集合 A 的一个关系与给出 $A\times A$ 的一个子集实质上一回事。

如上节中，例 2 关系对应的集合 S_R 由一切形如 (a,b) 的元素组成，其中 a 是 b 的后代；例 3 的 S_R的元素形如(a,b)，其中$|a|=|b|$；例 6 的 S_E 由一切$(a,a)(a\in A)$组成；例 7 中的 S_E 由一切适合$n|a-b$ 的整数对 (a,b) 组成。集合 A 的空关系显然对应 $A\times A$ 的空集 ϕ，而全关系对应的集合是整个 $A\times A$。

三、多个集合的积集

定义 2 设 A_1、A_2、…、A_n 是 n 个非空集合，一切形如$(a_1, a_2, \cdots, a_n)$的元素组合的集合，其中 $a_1\in A_1$，$a_2\in A_2$，$\cdots$，$a_n\in A_n$，称为积集 $A_1\times A_2\times\cdots\times A_n$。

例 3　设 $A=\{1, 2, 3\}$，$B=\{1, 2\}$，$C=\{a, b\}$，则

$$\begin{aligned}A\times B\times C=\{&(1,1,a),(1,1,b),(1,2,a),\\&(1,2,b),(2,1,a),(2,1,b),(2,2,a),\\&(2,2,b),(3,1,a),(3,1,b),(3,2,a),(3,2,b)\}.\end{aligned}$$

因子 A_i 也可以是无限个，不过本书不讨论无限积的情况。

四、商集

设集合 A 有一种分类，因而 A 表为不相交的类的并：

$$A=A_\alpha\cup A_\beta\cup\cdots.$$

每个类本来是 A 的一个子集，现在不把它们看成子集，而看成一个独立的元素，这些元素形成一个新的集合，称为集合 A 关于这种分类的商集合，记为 $\bar{A}$. A 中有多少类，$\bar{A}$ 就有多少元素.

上节知道，分类与等价关系是一致的，所以如果一开始给出的是集合 A 的一个等价关系，同样也可以定义商集合，这就是等价类组成的集合. 如果等价关系是 E，则商集合记为

$$\bar{A}=A/E.$$

商集合 $\bar{A}$ 看起来似乎就是 A，实际上，$\bar{A}$ 和 A 是两个绝然不同的集合，$\bar{A}$ 的元素是 A 中的类，而不是 A 的元素，这一点要分清(如图1—15、16).

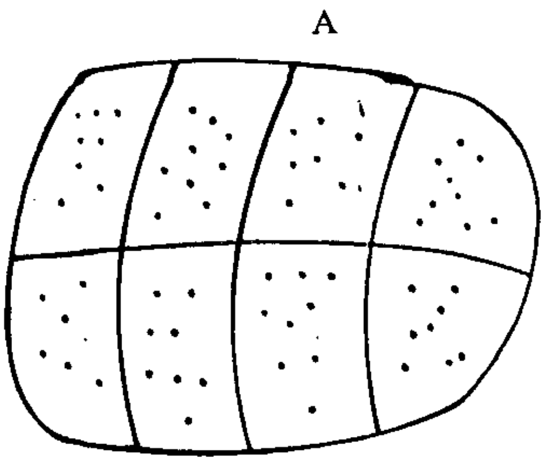


图 1—15

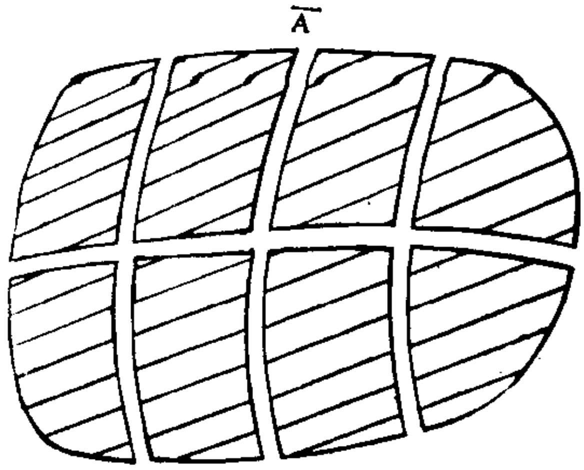


图 1—16

例 4 设 A 为某班全体学生组成的集合，假设班里学生又分成若干小组，规定 $a\,E\,b$ 当且仅当 a 与 b 同组，E 显

然是 A 的等价关系。每个小组是一个 E 等价类，商集 A/E 就是班里小组的集合。

例 5　同余是整数集 $\mathbf{Z}$ 的等价关系，以 n 为模的剩余类集 $\mathbf{Z}_n=\{[0],[1],\cdots,[n-1]\}$ 显然是 $\mathbf{Z}$ 关于同余关系的商集，即 $\mathbf{Z}_n=\mathbf{Z}/E$，其中 E 表示同余关系(见上节例 7 和五)。

例 6　由平面上所有点组成的集合 $\boldsymbol{R}_2$ 中，设 L 是一条固定直线，规定：aEb 当且仅当 a 和 b 在同一条平行于 L 的直线上。显然 E 是 $\boldsymbol{R}_2$ 的等价关系。每个 E 等价类是平行于 L 的一条直线。商集 $\boldsymbol{R}_2/E$ 是平面上的平行直线族(如图 1—17)，其元素是直线而不是点。

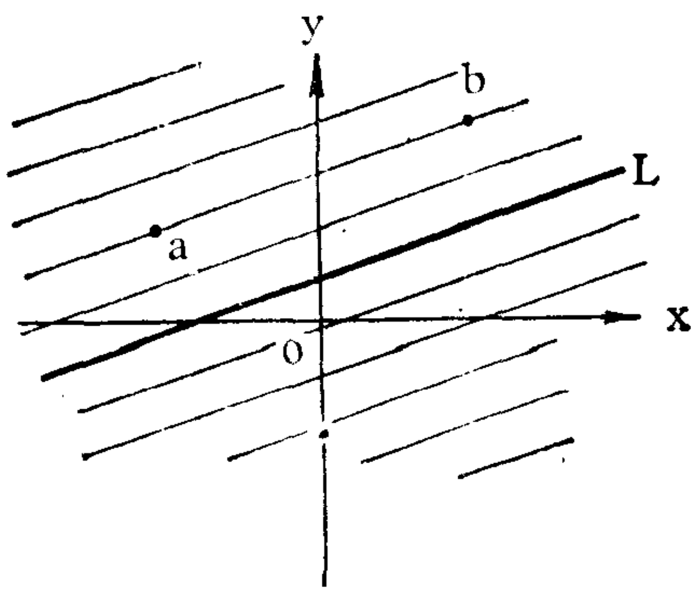


图 1—17

习　题　1·4

1. 设 $|A|=m$，$|B|=n$，求证 $|A\times B|=mn$。

2. 设 $|A|=n$，试将 A 分成两个不相交的集合 A_1、A_2，使 $|A_1\times A_2|$ 最大。

3．非负整数集 $\boldsymbol{N}$ 的下列关系在 $\boldsymbol{N}\times\boldsymbol{N}$ 中对应的子集是什么？

(1) $aRb \Longleftrightarrow a=b+1$；

(2) $aRb \Longleftrightarrow a=2b$；

(3) $aRb \Longleftrightarrow a$ 与 b 互素；

(4) $aRb \Longleftrightarrow 5\mid a-b$；

(5) $aRb \Longleftrightarrow 5\mid a+b$.

4．$A\times B$ 中，规定：$(a,b)E(c,d) \Longleftrightarrow b=d$．求证 E 是等价关系，且 $(A\times B)/E \sim B$.

5．设 σ 是 A 到 B 的满射，E 是习题1·3—3的关系 E，$\bar{A}=A/E$，求证 $\bar{A}\sim B$.

6．设 $m|n$．在 $\boldsymbol{Z}_n$ 中规定 $[a]E[b] \Longleftrightarrow m\mid a-b$．求证 E 是 $\boldsymbol{Z}_n$ 的等价关系，且 $\boldsymbol{Z}_m \sim \boldsymbol{Z}_n/E$.

7．设 $\boldsymbol{C}^*$ 是非零复数集，$\boldsymbol{R}^+$ 是正实数集，$U=[0,2\pi)\subset\boldsymbol{R}$．求证 $\boldsymbol{C}^*\sim\boldsymbol{R}^+\times U$．在 $\boldsymbol{C}^*$ 中规定 $z_1Ez_2 \Longleftrightarrow |z_1|=|z_2|$，则 E 是等价关系，$\boldsymbol{C}^*/E\sim U$．试证明之.

8．求证：

(1) $A\times(B\cup C)=(A\times B)\cup(A\times C)$；

(2) $A\times(B\cap C)=(A\times B)\cap(A\times C)$.

§1·5 代数运算

当我们学习数的时候，就几乎同时学习数的运算，若离开了运算，数也就没有什么价值了．设 a，b 是两个整数，$a-b$ 是由 a 与 b 唯一决定的一个整数，是 a 与 b 减法运算的结果．设 a，b 是两个非零有理数，则 $a\div b$ 是 a 和 b 唯一

决定的有理数，是 a 和 b 除法运算的结果.

数的运算加以抽象概括，可以得出一般集合中代数运算的概念.

定义 1 设 A 为非空集. 如果有一个法则 $\circ$，对于 A 中任意两个有序元素 a，b，由 $\circ$ 唯一确定 A 中的一个元素 $C=a\circ b$，则 $\circ$ 称为 A 的代数运算.

集合 A 的代数运算包括以下三个含义：

（1） A 的任意两个有序元素，都有运算结果；

（2） 运算结果仍在 A 中；

（3） 运算结果是唯一的.

例 1 设 $A=\{1, 2, 3\}$，规定 $a\circ b=a$，则 $\circ$ 是 A 的代数运算.

例 2 普通加法和乘法是正整数集 $\boldsymbol{P}$、实数集 $\boldsymbol{R}$ 的代数运算.

例 3 设 A 为非空集，A 的所有子集组成的子集族 $F(A)$ 中，集合的并与交都是 $F(A)$ 的代数运算.

例 4 设 $M_n(\boldsymbol{R})$ 是实 n 阶方阵的全体组成的集合，矩阵的加法和乘法都是它的代数运算.

例 5 $\boldsymbol{R}$ 中普通的除法不是代数运算，例如 $1, 0\in\boldsymbol{R}$，但 $1\div 0$ 没有运算结果，违反了(1).

例 6 非负整数集 $\boldsymbol{N}$ 中普通减法不是代数运算，例如 $1, 2\in\boldsymbol{R}$，但 $1-2=-1\overline{\in}\boldsymbol{N}$，违反了(2).

例 7 有理数集 $\boldsymbol{Q}$ 中如果规定 $\frac{b}{a}\circ\frac{d}{c}=\frac{b+d}{ac}$，则不是代数运算. 例如 $\frac{1}{2}$，$\frac{1}{3}\in\boldsymbol{Q}$，则一方面，

$$\frac{1}{2}\circ\frac{1}{3}=\frac{2}{6}=\frac{1}{3},$$

另一方面，

$$\frac{1}{2}=\frac{2}{4},\ \frac{1}{3}=\frac{2}{6},\ \frac{2}{4}\circ\frac{2}{6}=\frac{4}{24}=\frac{1}{6}\neq\frac{1}{3},$$

这就是说，同样一对元素，运算结果不是唯一的，违反了(3)。

从上面例子可以看出，代数运算并不与人们通常说的“运算”一样，如除法竟不是 $\boldsymbol{R}$ 的代数运算。

代数运算本身，并不要求有实际意义，同一集合可以同时规定许多代数运算，如 $\boldsymbol{Z}$ 中规定 $a\circ b=1$，$a\circ b=a^2$，$a\circ b=a+b^2-1$，$a\circ b=|a|-|b|+ab-2$ 等都是代数运算。

我们知道，集合 A 中两个有序的元素 a，b，可以看作积集 $A\times A$ 的一个元素 (a,b)，而 A 的代数运算是由一对有序的元素确定一个元素的法则，因而是 $A\times A$ 到 A 的一个映射。

这样，定义 1 可以改叙为更简捷的形式：

定义1′ 设 A 为非空集，$A\times A$ 到 A 的映射称为 A 的代数运算。

代数运算常用两种表达方式。

一种是利用表达式．这种方法适合代数运算有明显的规律的情况。

例如确定于 $\boldsymbol{R}$ 上的实二元函数表达式 $f(x,y)$，实际上确定 $\boldsymbol{R}$ 的一个代数运算，因由一对有序的实数 x，y，唯一确定一个实数 $f(x,y)$，它就是这一代数运算的结果。

如果代数运算规律不明显，则很难用表达式写出。如 $A=\{1,2,3\}$，定义代数运算“$\circ$”如下：$1\circ1=1$，$1\circ2$

$=2$，$1\circ 3=1$，$2\circ 1=2$，$2\circ 2=1$，$2\circ 3=3$，$3\circ 1=1$，$3\circ 2=3$，$3\circ 3=1$．这个代数运算可以用表给出，这是第二种表达代数运算的方法，称为运算表法或凯莱(Cayley)法.[注]

∘	1	2	3
1	1	2	1
2	2	1	3
3	1	3	1

表的最上一行和最左一列按相同次序写出 A 的全部元素，把 $a\circ b$ 写在 a 行 b 列的那个位置上。

这种方法适用于集合元素较少的情况.

习　题　1·5

1．下述法则是不是有理数集 Q 的代数运算？

(1) $a\circ b=\frac{1}{2}(a+b)$；

(2) $a\circ b=\frac{1}{2}[a(a+1)+b(b+1)]$；

(3) $a\circ b=a^2-2ab+b^2$；

(4) $a\circ b=\frac{b}{a}$；

(5) $a\circ b=b\sqrt{a}+2b^2$；

(6) $a\circ b=\sin a+\sin b$；

(7) $a\circ b=10^{a+b}$.

2．设 $A=\{1,2,3\}$．规定：$1\circ 2=1$，$1\circ 3=2$，$2\circ 1=2$，$2\circ 3=3$，$3\circ 1=1$，$3\circ 2=2$，$\circ$ 是否 A 的代数运算？

3．已知 $\circ$ 是集合 A 的代数运算，若规定 $a\,\bar{\circ}\,b=(a\circ b)$

注　A. Cayley (1821--1895)，英国数学家。

$\circ(a\circ b)$，证明$\bar{\circ}$也是A的代数运算。

4. 内积(数量积)是不是三维向量空间$\boldsymbol{R}_3$的代数运算？为什么？

5. 由两个元素组成的集合中，总共有多少种代数运算？

6. 设$S=\{a, b, c, d, e\}$，其运算表如下：

(1) 计算$b*d$，$c*c$和$[(a*c)*e]*a$；

(2) 计算$(a*b)*c$和$a*(b*c)$；

(3) 计算$(b*d)*c$和$b*(d*c)$。

*	a	b	c	d	e
a	a	b	c	d	e
b	b	c	a	c	c
c	c	a	b	b	a
d	d	b	b	e	a
e	d	b	a	d	c

本 章 提 要

一、集合：某些确定的元素的集体。

二、集合的运算：

1. $A\cup B=\{x|x\in A$ 或 $x\in B\}$；

2. $A\cap B=\{x|x\in A$ 且 $x\in B\}$；

3. $A\backslash B=\{x|x\in A$ 但 $x\overline{\in}B\}$。

三、映射：集合A到B的对应法则，使A的每个元素有B的唯一元素与之对应。

1. 单射——不同元素的象也不同的映射；

2. 满射——A的象集与B相等的映射；

3. 一一映射——是单射又是满射的映射。

四、关系：非空集合A中的法则R若对任意元素a和

b，aRb 或$a\bar{R}b$ 有且仅有一种成立，则 R 称为 A 的关系．具有反身性、对称性、传递性的关系称为等价关系．集合中给出一个等价关系与给出一种分类是一回事．

五、集合 A 与 B 的积集

$$A\times B=\{(a,\ b)\,|\,a\in A,\ b\in B\}.$$

六、集合 A 关于等价关系 E 的全体等价类作成的集合，称为 A 关于 E 的商集，即 A/E．

七、集合 A 的代数运算：即 $A\times A$ 到 A 的映射．

复 习 题 一

1．设 $f(x)$，$g(x)$是实多项式，其实根集合分别记为 A 和 B．求证：

（1）多项式 $f(x)g(x)$实根的集合为 $A\cup B$；

（2）多项式 $f^2(x)+g^2(x)$实根的集合为 $A\cap B$．

2．设$S_a=\{x\in\mathbf{R}\,|\,x\geqslant a\}$．求 $\bigcup\limits_{a} S_a$ 和 $\bigcap\limits_{a} S_a$．

3．设A，B，C 为三个集合．求证：

（1）$|A\cup B|=|A|+|B|-|A\cap B|$；

（2）$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|B\cap C|$
$-|C\cap A|+|A\cap B\cap C|$．

4．在整数集 $\mathbf{Z}$ 中规定 $\varphi(n)=r$，其中 r 是 5 除 n 的余数，$n=5q+r$，$0\leqslant r<5$．φ 是否 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的映射？$\varphi[\mathbf{Z}]=?$ φ 是否单射？$\varphi^{-1}[1]=?$

*5．设 $|A|=n$，$|B|=m$．A 到 B 有多少个不同的映射？

6．设 n 是固定的自然数，φ 是 $\mathbf{P}$ 的变换：$\varphi(k)$

$=\begin{cases} n-k, & (k<n); \\ n+k, & (k\geqslant n). \end{cases}$ φ 是否单射？满射？

7. 设 A 为[0, 1]上全体实函数组成的集合. φ 是 A 的变换，定义为 $\varphi(f(x))=(x^2+1)f(x)$. φ 是否单射？满射？

*8. 设 f 是 A 到 B 的映射，求证：

(1) f 是单射的充要条件为存在 B 到 A 的映射 g，使 gf 为 A 的恒等变换 ε_A.

(2) f 是满射的充要条件为存在 B 到 A 的映射 h，使 fh 为 B 的恒等变换 ε_B.

*9. 设 $A=\{1, 2, \cdots, n\}$，φ 是 A 的满射变换，要求 $\varphi(1)=i_1$，$\varphi(2)=i_2$，$\cdots$，$\varphi(k)=i_k$，$(k\leqslant n)$ 那末，这样的 φ 有多少？

10. 设 $A=B\cup C$，$B\cap C=\phi$，求证：$F(A)\sim F(B)\times F(C)$. 其中 $F(A)$ 表示 A 的子集族.

11. 设 φ 是 A 到 B 的满射，ψ 是 B 到 C 的满射，求证：$\psi\varphi$ 是 A 到 C 的满射. 对于单射或一一映射是否也有类似结果？

12. 设 $\{A_i \mid i\in I\}$ 是集合 A 的某些子集组成的集合，φ 是 A 的变换. 求证：

(1) $\varphi\left[\bigcup_{i\in I} A_i\right]=\bigcup_{i\in I}\varphi[A_i]$;

(2) $\varphi^{-1}\left[\bigcup_{i\in I} A_i\right]=\bigcup_{i\in I}\varphi^{-1}[A_i]$;

(3) $\varphi^{-1}\left[\bigcap_{i\in I} A_i\right]=\bigcap_{i\in I}\varphi^{-1}[A_i]$.

13. 设 φ 是 A 的一一变换，求证：φ 是恒等变换的充

要条件是 $\varphi\varphi=\varphi$。

*14. 设 φ 和 ψ 是正整数集 $\boldsymbol{P}$ 的变换；$\varphi(x)=2x$，$\psi(x)=2x-1$，试求变换 σ，使 $\sigma\varphi=\sigma\psi=\varepsilon_p$。

*15. n 元集中最多有多少种关系和代数运算？

第二章　群胚与半群

本章介绍群胚和半群的基本概念和性质，为下面学习群、环作准备.

§2·1　群胚和半群的概念

一、群胚

假设非空集合A有一个代数运算（见§1·5），这个代数运算叫什么名字，用什么符号表示是无关紧要的，我们不妨叫它为“乘法”，记为“·”（也可省去运算符号），这时，称A关于·构成群胚，记为$\langle A, \cdot\rangle$．其中A表示群胚所含元素的集合，·表示代数运算的法则．如果这个代数运算已有习惯的名称和符号，也可维持原有的名称和符号．同一集合A对不同的代数运算形成的群胚并不相同，但在不致产生混淆的情况下，可以把群胚$\langle A, \cdot\rangle$简记为A.

二、半群

群胚是带有一个代数运算的集合，至于这个代数运算的性质并无任何要求．下面引进一种特殊群胚——半群.

定义1　设$\langle A, \cdot\rangle$是一个群胚，如果对于任意的$a, b, c\in A$，都有

$$(ab)c = a(bc), \tag{1}$$

则称$\langle A,\cdot\rangle$为半群.

就是说，半群是适合结合律的群胚.

例1 由数组成的集合按普通数的加法或乘法作成的群胚，都是半群.

这是因为数的加法和乘法都适合结合律.

例2 设$A=\{a_1,a_2\}$,其乘法表如下：

$\cdot$	a_1	a_2
a_1	a_2	a_1
a_2	a_1	a_2

求证$\langle A,\cdot\rangle$为半群.

证明：为了验证(1)式，须考虑8种情况：

$$(a_1a_1)a_1=a_1=a_1(a_1a_1),$$
$$(a_1a_1)a_2=a_2=a_1(a_1a_2),$$
$$(a_1a_2)a_1=a_2=a_1(a_2a_1),$$
$$(a_1a_2)a_2=a_1=a_1(a_2a_2),$$
$$(a_2a_1)a_1=a_2=a_2(a_1a_1),$$
$$(a_2a_1)a_2=a_1=a_2(a_1a_2),$$
$$(a_2a_2)a_1=a_1=a_2(a_2a_1),$$
$$(a_2a_2)a_2=a_2=a_2(a_2a_2).$$

所以，$\langle A,\cdot\rangle$是半群.

例3 设A为任意非空集，规定$ab=a$，则$\langle A,\cdot\rangle$是半群.

证明：$\langle A,\cdot\rangle$显然是群胚.

任取a、b、$c\in A$，则

$$(ab)c=ac=a,$$
$$a(bc)=ab=a.$$

因而$(ab)c=a(bc)$，$\langle A,\cdot\rangle$是半群.

例4 实多项式集$\boldsymbol{R}[x]$关于多项式的加法和乘法都适合结合律，所以$\langle \boldsymbol{R}[x],+\rangle$和$\langle \boldsymbol{R}[x],\cdot\rangle$是半群.

例 5 实 n 阶方阵集 $M_n(\boldsymbol{R})$ 关于矩阵的加法和乘法都适合结合律，所以 $\langle M_n(\boldsymbol{R}), +\rangle$ 和 $\langle M_n(\boldsymbol{R}), \cdot\rangle$ 是半群。

例 6 在正整数集 $\boldsymbol{P}$ 中，任意 a、b 都有唯一的最大公因数和最小公倍数，这样就决定了 $\boldsymbol{P}$ 中两个代数运算：

$$a \circ b = (a, b),$$

$$a * b = [a, b].$$

由自然数的性质，可以证明

$$((a,b),c) = (a,(b,c)),$$

$$[[a,b],c] = [a,[b,c]].$$

因而，$\langle \boldsymbol{P}, \circ\rangle$ 和 $\langle \boldsymbol{P}, *\rangle$ 都是半群。

例 7 在以 n 为模的剩余类集 $\boldsymbol{Z}_n$（见 §1·3）中，规定

$$[a] + [b] = [a+b], \tag{2}$$

$$[a][b] = [ab]. \text{注} \tag{3}$$

求证 $\langle \boldsymbol{Z}_n, +\rangle$ 和 $\langle \boldsymbol{Z}_n, \cdot\rangle$ 都是半群。

证明：首先证明 $\langle \boldsymbol{Z}_n, +\rangle$ 和 $\langle \boldsymbol{Z}_n, \cdot\rangle$ 是群胚，即 $+$ 和 $\cdot$ 是 $\boldsymbol{Z}_n$ 的代数运算。

因为对于任意的 $[a], [b] \in \boldsymbol{Z}_n$，$[a+b]$ 和 $[ab]$ 都在 $\boldsymbol{Z}_n$ 中，下面只须证明运算结果是唯一的，即如果 $[a] = [a_1]$，$[b] = [b_1]$，则有

$$[a+b] = [a_1 + b_1], [ab] = [a_1 b_1].$$

事实上，如 $[a] = [a_1]$，$[b] = [b_1]$，即 a 与 a_1 同余，b 与 b_1 同余，则 $n \mid a - a_1$，$n \mid b - b_1$，因而 $(a+b) - (a_1 + b_1) = (a - a_1) + (b - b_1)$ 是 n 的倍数，故 $a+b$ 与 $a_1 + b_1$ 同余，

注 (2)式表明，a 所在类与 b 所在类的和规定为 $a+b$ 所在的类，如 $[2]+[3]=[5]$。(3)式的意义类似。$[a]$ 中元素不只是 a，$[b]$ 中元素不只是 b，为证(2)，(3)是代数运算，须证(2)，(3)都与代表元选取无关，即运算结果是唯一的。

$[a+b]=[a_1+b_1]$.

另一方面，

$$\begin{aligned}&ab-a_1b_1\\=&ab-ab_1+ab_1-a_1b_1\\=&a(b-b_1)+b_1(a-a_1)\end{aligned}$$

也是 n 的倍数，故 ab 与 a_1b_1 同余，$[ab]=[a_1b_1]$。

下面证明 $\mathbf{Z}_n$ 关于 + 和 · 都适合结合律。

事实上，任取$[a]$、$[b]$、$[c]\in\mathbf{Z}_n$，则

$$\begin{aligned}&[a]+([b]+[c])\\=&[a]+[b+c]\\=&[a+(b+c)]\\=&[(a+b)+c]\\=&[a+b]+[c]\\=&([a]+[b])+[c].\end{aligned}$$

$$\begin{aligned}&([a][b])[c]\\=&[ab][c]\\=&[(ab)c]\\=&[a(bc)]\\=&[a][bc]\\=&[a]([b][c]).\end{aligned}$$

所以，$\langle\mathbf{Z}_n,+\rangle$和$\langle\mathbf{Z}_n,\cdot\rangle$都是半群。

例 8 非空集 S 的所有子集组成的集合族 $F(S)$ 中，集合的并集($\cup$)与交集($\cap$)运算都适合结合律(见 §1·1 定理 1(3))，所以$\langle F(S),\cup\rangle$和$\langle F(S),\cap\rangle$都是半群。

例 9 $\mathbf{R}$ 中规定 $a\circ b=\dfrac{a+b}{2}$。则 $\langle\mathbf{R},\circ\rangle$虽是群胚，但不

是半群。

事实上，$(1\circ2)\circ3=\frac{1+2}{2}\circ3=\frac{\frac{3}{2}+3}{2}=\frac{9}{4}$，$1\circ(2\circ3)$ $=1\circ\frac{2+3}{2}=\frac{1+\frac{5}{2}}{2}=\frac{7}{4}$，所以$\circ$不适合结合律。

三、子群胚和子半群

一个群胚的非空子集，如果关于原群胚的乘法仍然构成群胚，则称为原群胚的子群胚。

显然，群胚的非空子集作成子群胚的充要条件是这个子集关于原乘法封闭(所谓封闭，是指这个子集的任意两元素的积还在该子集中)。

一个半群的非空子集，如果关于原半群的乘法仍然构成半群，则称为原半群的子半群。

由于半群中元素的乘法适合结合律，所以半群的非空子集是子半群的充要条件是它关于原乘法封闭。

例如正偶数集和正奇数集关于数的乘法都是正整数乘半群；常数项为零的实多项式集合关于多项式加法和乘法是$\langle \boldsymbol{R}[x],+\rangle$和$\langle \boldsymbol{R}[x],\cdot\rangle$的子半群；$n$阶实非退化方阵集合$M_n^*(\boldsymbol{R})$作成$\langle M_n(\boldsymbol{R}),\cdot\rangle$的子半群，但不是$\langle M_n(\boldsymbol{R}),+\rangle$的子半群，因为两个非退化方阵之和可以是退化的。

在半群中由于有结合律，n个元素的乘积与加括号方式无关(但不能交换因子次序)，如$((a_1a_2)a_3)a_4=(a_1a_2)(a_3a_4)=(a_1(a_2a_3))a_4=a_1(a_2(a_3a_4))=a_1((a_2a_3)a_4)$，所以写成$a_1a_2a_3a_4$是有意义的。这一事实可用归纳法证实。在半群中元素的

方幂规定为：$a^n=a^{n-1}\cdot a$，$a^1=a(n>1)$．易证

$$a^n\cdot a^m=a^{n+m},\ (a^n)^m=a^{nm}\ (m,n>0).$$

如果半群中任意两个元素可换($ab=ba$)，则称为可换半群，在这种半群中n个元素的乘积不仅与括号方式无关，也与因子次序无关．如数或多项式组成的半群多是可换半群．例3和例5中$\langle M_n(\boldsymbol{R}),\cdot\rangle$不是可换半群．

习 题 2·1

1．设$\langle A,\cdot\rangle$和$\langle B,\circ\rangle$都是群胚，在积集$A\times B$中规定$(a,b)*(a_1,b_1)=(a\cdot a_1,b\circ b_1)$，则$\langle A\times B,*\rangle$是群胚．试证明之．

2．上题中将"群胚"改为"半群"仍成立．试证明之．

3．下列集合关于相应的代数运算是否作成半群？为什么？

(1) $\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\}$

关于矩阵乘法；

(2) $\{z\in\boldsymbol{C}\mid |z|=1\}$关于数的除法；

(3) $\{a+b\sqrt{2}\mid a、b\in\boldsymbol{Q}\}$关于数的加法；

(4) $\{a+bi\mid a、b\in\boldsymbol{R}^+\}$关于复数的乘法；

(5) 以1为根的实多项式集合关于多项式乘法．

4．求证：

(1) 半群A是自身的子半群；

(2) 半群A的两个子半群的交如果非空，则是A的子半群；

(3) 如果B是半群A的子半群，则B的子半群C也是

A的子半群。

5. 如果A是半群，则A中单元素a构成子半群的充要条件是a适合：$a^2=a$。

6. 下面是一个半群的乘法表，试将空白处填上元素：

·	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	d	c	d
d				

7. 设$A=\{a_1,a_2\}$，试在A中建立两个半群。用乘法表给出。

8. 上题各半群中有哪些子半群？

9. 设S是非空集，S的全体变换构成的集合记为$\mathbf{S}(S)$,求证$\mathbf{S}(S)$关于变换的乘法作成半群。

10. 设$T\subseteq S$，求证：$\langle F(T),\cup\rangle$是$\langle F(S),\cup\rangle$的子半群；$\langle F(T),\cap\rangle$是$\langle F(S),\cap\rangle$的子半群。其中$F(T)$、$F(S)$表示T、S的所有子集组成的集合族。

11. 写出下列半群的乘法表：

(1) $\langle S,\circ\rangle$,其中$S=\{1,2,3,4,6,12\}$,$a\circ b=(a,b)$；

(2) $\langle S,*\rangle$,其中$a*b=[a,b]$；

(3) $\langle F(\bar{S}),\cap\rangle$,其中$\bar{S}=\{1,2,3\}$；

(4) $\langle F(\bar{S}),\cup\rangle$。

§ 2·2 半群的整除性

这一节讨论半群中元素整除的性质，以及与整除性有关的一些特殊元素，如单位元、零元、可逆元等.

一、整除性

我们知道，所谓整数 a 整除整数 b，是指存在整数 c，使 $ca=b$。整除的概念可以推广到半群中去.

定义 1 设 a、b 是半群 $\langle A,\cdot\rangle$ 的元素，如果存在 $c\in A$，使 $ac=b$，则称 a 为 b 的左因子，或称 a 左整除 b；如果存在 $d\in A$，使 $da=b$，则称 a 是 b 的右因子，或称 a 右整除 b；如果 a 同时是 b 的左因子和右因子，那末称 a 是 b 的因子，或称 a 整除 b，记为 $a|b$.

如果 a 是 b 的左(右)因子，b 是 c 的左(右)因子，则显然 a 是 c 的左(右)因子.

二、单位元

某些半群中存在着类似于数集中 1 那样的元素，它乘任意元素，都使这个元素不变.

定义 2 半群 $\langle A,\cdot\rangle$ 中，如有元素 e_l，它左乘半群中的每个元素 a 的积仍是 a，即

$$e_l a=a,(a\in A)$$

则称 e_l 是 $\langle A,\cdot\rangle$ 的左单位元.

同样可以定义右单位元 e_r.

如果 e 既是左单位元又是右单位元，则称为半群的单位

元．（本书通常用 e 表示一般半群的单位元）

显然，半群的左(右)单位元是半群的所有元素的左(右)因子．

在半群 $\langle \boldsymbol{N},\cdot\rangle$、$\langle \boldsymbol{Z},\cdot\rangle$、$\langle \boldsymbol{Q},\cdot\rangle$、$\langle \boldsymbol{R},\cdot\rangle$、$\langle \boldsymbol{C},\cdot\rangle$中，数1是单位元；而在 $\langle \boldsymbol{N},+\rangle$、$\langle \boldsymbol{Z},+\rangle$、$\langle \boldsymbol{Q},+\rangle$、$\langle \boldsymbol{R},+\rangle$、$\langle \boldsymbol{C},+\rangle$中，数0是单位元．

§2·1 例2的半群$\langle A,\cdot\rangle$中，a_2 显然是单位元．例3的半群$\langle A,\cdot\rangle$中，每个元素都是右单位元，因为对每个 $a\in A$，等式

$$xa=x$$

对所有 $x\in A$ 成立．但只要A至少含两个元素，那就没有左单位元．事实上，任取 $a\in A$，设 $b\neq a$，则

$$ab=a\neq b,$$

说明 a 不是左单位元．

全体实 n 阶方阵组成的加半群$\langle M_n(\boldsymbol{R}),+\rangle$中，零方阵是单位元，而乘半群$\langle M_n(\boldsymbol{R}),\cdot\rangle$的单位元是单位方阵．

半群$\langle F(S),\cup\rangle$中（§2·1 例8）、ϕ 是单位元；而半群$\langle F(S),\cap\rangle$的单位元是 S．事实上，对于任意 $T\in F(S)$（即 $T\subseteq S$），总有

$$\phi\cup T=T\cup\phi=T,$$

$$S\cap T=T\cap S=T.$$

半群可以有许多左(右)单位元，也可以没有左(右)单位元．如 $\boldsymbol{Z}$ 中，规定 $a\circ b=b$，那末每个整数 a 都是$\langle \boldsymbol{Z},\circ\rangle$这个半群的左单位元，因而有无穷多个左单位元．全体偶数按普通乘法作成半群，它显然既无左单位元，也无右单位元．

定理1 半群$\langle A,\cdot\rangle$如果同时存在左单位元 e 和右单位

元 f，则 $e=f$.

证明：e 是左单位元，所以 $ef=f$；而 f 是右单位元，所以 $ef=e$. 因而 $e=f$.

证毕

推论 1 半群中至多有一个单位元.

证明：设 e 和 f 都是单位元. 自然，e 是左单位元，f 是右单位元，由定理 1，$e=f$.

三、零元

数的乘半群中，数 0 也是特殊的元素，任何数与它相乘，其积都等于 0 本身. 许多半群中也有这种性质的元素.

定义 3 半群 $\langle A, \cdot\rangle$ 中，如有元素 0_l，它左乘半群的每个元素 a 的积，都等于 0_l，即

$$0_l a = 0_l, (a \in A)$$

则称 0_l 是 $\langle A, \cdot\rangle$ 的左零元.

同样可以定义右零元 0_r.

如果 0 既是左零元又是右零元，则称为半群的零元.

显然，半群的每个元素是左(右)零元的右(左)因子.

半群 $\langle \boldsymbol{R}, +\rangle$ 中没有左零元或右零元. 事实上，假如 a 是其左零元，则对于任何 $x \in \boldsymbol{R}$，总有 $a+x=a$，推出 $x=0$ (指数零)，与 x 的任意性矛盾. 由于加法是适合交换律的，所以这个半群也无右零元.

同理，$\langle \boldsymbol{Z}, +\rangle$、$\langle \boldsymbol{Q}, +\rangle$、$\langle \boldsymbol{C}, +\rangle$ 以及 $\langle \boldsymbol{P}, +\rangle$、$\langle \boldsymbol{Q}^+, +\rangle$、$\langle \boldsymbol{R}^+, +\rangle$ 等都没有左零元或右零元.

半群 $\langle \boldsymbol{R}, \cdot\rangle$ 有零元——数 0，数 0 也是 $\langle \boldsymbol{Z}, \cdot\rangle$、$\langle \boldsymbol{Q}, \cdot\rangle$、$\langle \boldsymbol{C}, \cdot\rangle$、$\langle \boldsymbol{N}, \cdot\rangle$ 等半群的零元.

在§2·1例3的半群中，任取$a\in A$，则等式$ax=a$对任意$x\in A$成立，即每个元素都是左零元。只要$|A|>1$，则$\langle A,\cdot\rangle$就无右零元。

$\langle M_n(\boldsymbol{R}),\cdot\rangle$的零元是零方阵。

$\langle F(S),\cup\rangle$的零元是S，$\langle F(S),\cap\rangle$的零元是ϕ。事实上，对于$T\in F(S)$（即$T\subseteq S$）总有

$$S\cup T=T\cup S=S,$$

$$\phi\cap T=T\cap\phi=\phi.$$

与定理1对偶的是

定理2 半群$\langle A,\cdot\rangle$中如果同时存在左零元0_l和右零元0_r，则$0_l=0_r$。

证明：$0_l0_r=0_l$，又$0_l0_r=0_r$，故$0_l=0_r$。

证毕

推论2 半群中至多有一个零元。

除单元素半群外，半群的单位元不会与零元重合。事实上，假若$0=e$，对于任意元素x，有

$$0x=x0=0,$$

$$ex=xe=x,$$

得到$e=0=x$，即所有元素相互重合。

四、逆元

在有理数乘半群$\langle \boldsymbol{Q},\cdot\rangle$中，1是单位元，对于任何非零有理数$a$，存在$a^{-1}\in\boldsymbol{Q}$，使

$$aa^{-1}=a^{-1}a=1.$$

许多半群也具有上述性质的元素。

定义4 设$\langle A,\cdot\rangle$是具有单位元e的半群，$a\in A$。如果

存在元素 b，使 $ba=e$，则称 b 是 a 的左逆元；如果存在元素 c，使 $ac=e$，则称 c 是 a 的右逆元；如果存在元素 a^{-1}，使 $a^{-1}a=aa^{-1}=e$，则称 a^{-1} 为 a 的逆元(约定 a^{-1} 永远代表元素 a 的逆元)．具有逆元的元素，称为可逆元，或简称其可逆．

具有单位元的半群，总有可逆元，因为单位元本身就是一个可逆元．无单位元的半群自然不会有可逆元，以下我们假定半群都有单位元．先来介绍判别可逆元的两个准则：

定理 3 半群中元素可逆的充要条件为它是单位元的因子．

证明：如果 a 可逆，则 $a^{-1}a=aa^{-1}=e$，即 $a|e$；反之，如果 $a|e$，则有 b，c，使 $ab=ca=e$，因而 $b=eb=(ca)b=c(ab)=ce=c$．即 $b=c=a^{-1}$．

证毕

定理 4 半群中元素可逆的充要条件为它是半群所有元素的因子．

证明：如果 a 可逆，则 $a|e$，但 e 整除所有元素，因而 a 也整除所有元素；反之，如果 a 整除所有元素，当然也整除 e，由上一定理知，a 可逆．

证毕

在半群$\langle \boldsymbol{Q},\cdot\rangle$、$\langle \boldsymbol{R},\cdot\rangle$、$\langle \boldsymbol{C},\cdot\rangle$中，所有非零数都是可逆元，因为 $a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$．零不是可逆元，因为我们有

定理 5 在非单元素半群中，零元是不可逆元．注

证明：设 0 是零元，如果有逆元 0^{-1}，则

注 单位元与零元在单元素半群$\langle a\rangle$中，都是 a．

$$00^{-1}=0^{-1}0=e.$$

根据零元的定义，

$$00^{-1}=0^{-1}0=0,$$

因而 $0=e$，矛盾。

证毕

可逆元总有逆元，那末它有多少逆元呢？

定理 6 半群中可逆元的逆元是唯一的。

证明： 设 b 和 c 都是 a 的逆元，则

$$ab=ba=e,$$

$$ac=ca=e.$$

于是，$b=eb=(ca)b=c(ab)=ce=c$.

证毕

定理 7 半群中的可逆元集作成子半群.

证明： 设 $G(A)$是半群 A 的可逆元集，$e\in G(A)\neq\phi$. 设 $a,b\in G(A)$，则 $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aa^{-1}=e$，同理$(b^{-1}a^{-1})(ab)=e$，即 ab 可逆，或说 $ab\in G(A)$.$G(A)$关于乘法封闭，即作成子半群.

证毕

$G(A)$ 不仅对于乘法封闭，关于求逆也封闭，因如果 $a\in G(A)$，$a^{-1}a=aa^{-1}=e$，则说明 a^{-1} 可逆，$a^{-1}\in G(A)$. $G(A)$是半群 A 的重要子半群，在以后的讨论中还要提及.

半群$\langle \mathbf{R}[x],\cdot\rangle$的单位元是 1，可逆元集由全体零次多项式组成(即$\mathbf{R}^*$).

$\langle M_n(\mathbf{R}),\cdot\rangle$中可逆元集由全体 n 阶非退化方阵组成，因为方阵可逆的充要条件为非退化.

半群$\langle F(S),\cup\rangle$和$\langle F(S),\cap\rangle$的可逆元集最简单，前者

只有单位元ϕ本身，后者只有单位元S本身。

五、从运算表中观察到什么？

假设$A=\{a,b,c,d\}$。给出A的乘法如表所示：

$\cdot$	a	b	c	d
a	a	c	c	a
b	c	b	c	b
c	c	c	c	c
d	a	b	c	d

易证$\langle A,\cdot\rangle$是半群。

我们以它为例，说明如何从运算表中看出元素的整除性、半群的单位元、零元、可逆元以及可换性。

1．整除性：第一行只有a和c两个元素，所以a是a的左因子，但a不是b或d的左因子，因a无论左乘什么元素也不等于b或d。第一列中，只有a和c两个元素，所以a也是a和c的右因子，不是b或d的右因子。同理，b是c和b的因子，不是a或d的因子；c是c的因子，不是a，b，d的因子；d是a，b，c，d的因子。

2．单位元：左单位元从左面乘任意元素，等于这一元素，所以，与最上一行完全相同的行对应的最左边的元素，就是左单位元。易见，d是左单位元。同样道理，可以推知d也是右单位元，因而是单位元。

3．零元：左零元从左边乘任意元素都应等于左零元本身。所以表中如果有一行从左到右都是同一元素，那末这个元素即左零元。同样，从列可以判断右零元。易见，c是左

零元也是右零元，即零元.

4. 可逆元：既然 d 是单位元，只要找出乘积是 d 的元素便可找出互逆的元素. 如 $xy=d$，那末 x 是 y 的左逆元，y 是 x 的右逆元. 从表上可见，只有 $dd=d$，即 d 是唯一的可逆元.

5. 可换性：乘积 ab 与 ba 刚好处于表中对称位置，其对称轴是左上角到右下角的对角线. 半群可换当且仅当其乘法表关于上述对角线对称. 不难看出，这个半群是可换的.

习 题 2·2

1. 求证：在半群 A 中，如果 b 是 a 的左因子，则对任意的 $x\in A$，b 是 ax 的左因子.

2. 求证：在半群 $\langle F(S),\cup\rangle$ 中，$T|W$ 当且仅当 $T\subseteq W$；在半群 $\langle F(S),\cap\rangle$ 中，$T|W$ 当且仅当 $W\subseteq T$.

3. 在 §2·1 例 6 的半群 $\langle \boldsymbol{P},\circ\rangle$ 中，求证：

(1) $a|b$ 当且仅当在通常的意义下 b 整除 a；

(2) 没有单位元；

(3) 零元是 1 .

在半群 $\langle \boldsymbol{P},*\rangle$ 中相应的结果是什么？

4. 求证：半群的可逆元互相整除，可逆元的因子也是可逆元.

5. 求证：半群的左零元构成子半群.

6. 求证：半群的左单位元构成子半群.

7. 在半群中，是否总有 $a|a$？举例说明.

8. 求证：半群中，能被一切元素整除的元素如果存在，则这样元素的全体作成子半群.

9. 设$\langle A, \cdot\rangle$是半群，$u \notin A$，设 $B=A\cup\{u\}$. 在 B 中规定乘法如下：

$$a\circ b=\begin{cases}a\cdot b, & \text{当 } a,b\in A \text{ 时；}\\ a, & \text{当 } b=u \text{ 时；}\\ b, & \text{当 } a=u \text{ 时。}\end{cases}$$

求证：$\langle B,\circ\rangle$是有单位元的半群.

10. 设$\langle A, \cdot\rangle$是半群，$v\notin A$，设 $C=A\cup\{v\}$. 在 C 中规定乘法如下：

$$a*b=\begin{cases}a\cdot b, & \text{当 } a,b\in A \text{ 时；}\\ a, & \text{当 } a=v \text{ 时；}\\ b, & \text{当 } b=v \text{ 时。}\end{cases}$$

求证：$\langle C,*\rangle$是有零元的半群.

11. 试分析§2·1各例中元素整除的实际意义.

§2·3　唯一分解半群

这一节介绍半群的因子分解理论，即考虑元素分解为既约元之积的问题，包括能否分解和分解是否唯一两个方面. 为此，须引进可消半群、相伴元、既约元、唯一分解半群的概念.

一、可消半群

如果 a，x，y 都是非零数，满足

$$ax=ay，\text{或者 } xa=ya，$$

则两端可以消去 a，得 $x=y$. 这是大家熟悉的消去律. 消去律在一般的半群中，并不一定成立，如在半群$\langle \mathbf{Z}_6,\cdot\rangle$中，

$$[3][2]=[6]=[12]=[3][4],$$

但$[2]\neq[4]$。

定义1 设$\langle A,\cdot\rangle$是半群，如果在A中适合消去律，即由等式$ax=ay$或由等式$xa=ya$都可推出$x=y$，则称此半群为可消半群。

如非零数组成的乘半群、非零实多项式$R^*[x]$关于多项式乘法都作成可消半群。至少含两个元素的半群，如果有左零元或右零元，则不是可消半群。事实上，设0_l是左零元，$x\neq y$，但有$0_lx=0_l=0_ly$。同样的讨论适用于右零元。

在可消半群中，方程$ax=b$或$ya=b$都至多有一个解。事实上，设x_1，x_2都是$ax=b$的解，则$ax_1=ax_2(=b)$，由消去律，$x_1=x_2$。

二、相伴元

本节以下将假定$\langle A,\cdot\rangle$是有单位元e的可换可消半群。

定义2 在有单位元的可换可消半群A中，如果a和b互相整除，则称b是a的相伴元，或称a与b相伴。

如在半群$\langle \mathbf{Z}^*,\cdot\rangle$中，$a$与$-a$相伴。在半群$\langle R^*[x],\cdot\rangle$中，$f(x)$与$rf(x)$相伴，这里$r$是任意非零实数。

相伴显然是A中的关系，它还是等价关系。事实上，对于$a\in A$，$a=ae=ea$，所以a与自身相伴，即反身性成立。如果a与b相伴，即a与b互相整除，自然b与a也相伴，对称性成立。如果a与b相伴，b与c相伴，即a与b互相整除，b与c互相整除，由整除的传递性，a与c也互相整除，即a与c相伴，传递性成立。

等价关系决定分类，于是在A中就有若干相伴类。如

$\langle Z^*, \cdot\rangle$中，$\{1, -1\}, \{2, -2\}, \cdots$都是相伴类. 在$\langle R^*[x], \cdot\rangle$中，每个相伴类形如$\{rf(x) \mid r\in R^*\}$. 即同一类中的多项式系数成比例.

下面，考虑一般情况下相伴类的结构.

定理 1 A中a与b相伴的充要条件是存在可逆元c，使$a=bc$。

证明：设$a=bc$，c可逆。一方面有$b|a$，另一方面，因为$b=ac^{-1}$，故$a|b$。即a与b相伴.

反之，设a与b相伴. 由$b|a$，知存在c，使$a=bc$。又因$a|b$，故有d，使$b=ad$，因而$ae=a=a(dc)$。A是可消可换半群，所以$e=dc=cd$，$d=c^{-1}$，c是可逆元.

证毕

这个定理告诉我们，一个元素a所在的相伴类$[a]$由a与所有可逆元的乘积组成，即

$$[a]=\{ar \mid r\in G(A)\},$$

其中$G(A)$表示A的可逆元集.

在$\langle Z^*, \cdot\rangle$中，可逆元集是$\{1, -1\}$，故$[a]=\{a, -a\}$。在$\langle R^*[x], \cdot\rangle$中，可逆元集是$R^*$，故有$[f(x)]=\{rf(x) \mid r\in R^*\}$. 与前面的结果一致.

那末，可逆元所在的相伴类是怎样的呢？

定理 2 A的所有可逆元作成同一个相伴类.

证明：任取可逆元a，只须证明$[a]=G(A)$. 由定理1，$[a]=\{ag \mid g\in G(A)\}$。$ag$也是可逆元（§2·2定理7），故$ag\in G(A)$，$[a]\subseteq G(A)$。反之，设$h$是可逆元，取$g=a^{-1}h$，$g$也是可逆元。$h=a(a^{-1}h)=ag\in[a]$。因而$G(A)\subseteq[a]$。即$G(A)=[a]$。

证毕

相伴类有一个有趣的性质是一般分类没有的：

定理 3 A 的任何两个相伴类等势.

分析：须证任意相伴类与 $G(A)$ 有一一对应.

证明：任取相伴类 $[a]$. 由定理 1，$[a]=\{ag\mid g\in G\}$. 取 $[a]$ 到 $G(A)$ 的对应法则 σ 如下：

$$\sigma(ag)=g.$$

σ 是映射. 事实上，如果 $ag_1=ag_2$，由消去律，$g_1=g_2$，即 $\sigma(ag_1)=\sigma(ag_2)$.[注] 此外，$\sigma$ 显然是满射. σ 是单射，事实上，若 $ag_1\neq ag_2$，可知 $g_1\neq g_2$，即 $\sigma(ag_1)\neq\sigma(ag_2)$. 所以 σ 是一一映射，$[a]\sim G(A)$.

证毕

三、既约元

A 的任意元素 a 至少有以下两种因子：A 的可逆元和 a 的相伴元. 这两种因子称为 a 的平凡因子，其他因子称为 a 的真因子.

如 $\langle \mathbf{Z}^*,\cdot\rangle$ 中，2 只有平凡因子 ±1（可逆元）、±2.（相伴元），但 4 除平凡因子 ±1、±4 外，还有真因子 ±2.

$\langle \mathbf{R}^*[x],\cdot\rangle$ 中，$x+1$ 只有平凡因子 r 和 $r(x+1)$（其中 $r\in\mathbf{R}^*$），但 x^2-1 除平凡因子外，还有真因子 $r(x+1)$ 及 $r(x-1)$（$r\in\mathbf{R}^*$）.

定义 3 在有单位元的可换可消半群 A 中，一个非可逆

注 要证 A 到 B 的对应法则 σ 是映射，本来应证：A 的任意元素都有象，象全部在 B 中；象是唯一的. 一般前两条可从法则 σ 直接看出，只须证明唯一性.

元 a 如果有真因子，则称为可约元，否则，称为既约元。

既约元是整数中的不可分解数(即正负素数)及多项式中不可约多项式等概念的推广。

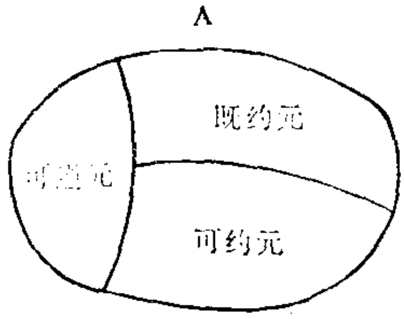


图 2—1

A 的元素分为三大类：可逆元、可约元和既约元。可逆元既不是可约元，也不是既约元（如图 2—1)。某些半群只有可逆元，没有可约元和既约元，如$\langle Q^*,\cdot\rangle$，单位元是 1，每个元素$\frac{b}{a}$都可逆，其逆元是$\frac{a}{b}$。

定理 4 A 中既约元的相伴元也是既约元。

证明：设 q 与既约元 p 相伴，$q=p\varepsilon$,其中 ε 是可逆元。q 不是可逆元，否则推出 $p=q\varepsilon^{-1}$ 是可逆元。如果 q 可约，设 $q=ab$，a 和 b 是 q 的真因子，则 $ab=p\varepsilon, p=a(b\varepsilon^{-1})$。因为 p 是既约元，故 a 和 $b\varepsilon^{-1}$ 是 p 的平凡因子，即或是可逆元，或是 p 的相伴元。分两种情况：

如果 a 是可逆元，则 $b\varepsilon^{-1}$是 p 的相伴元，而 b 与 $b\varepsilon^{-1}$ 相伴，从而与 p 相伴，因此与 $p\varepsilon=q$ 相伴，是 q 的平凡因子，矛盾。

如果 a 是 p 的相伴元，则也是 $q=p\varepsilon$ 的相伴元，而 $q=ab$，由定理 1，b 是可逆元，是 q 的平凡因子，也推出矛盾。

所以，q 是既约元。

证毕

定理 5 A 中可约元的相伴元也是可约元。

证明：设 $a\in A$ 是可约元，b 是 a 的相伴元。如果 b 是可逆元或既约元，由定理 4 和定理 2，a 是可逆元或既约元，

不是可约元。所以 b 是可约元。

证毕

所以，可逆、既约、可约的性质，不会打破相伴类的界限，是一个相伴类的元素整体的性质。

四、唯一分解半群

在多项式代数中知道，任意非零实多项式，总可以分解为不可约多项式的乘积，而且多项式的任意两种分解，因式个数总相等，并且适当交换因式的次序后，对应的因式至多相差一个非零常数因子。上面说过，相差一个非零常数因子的多项式相伴，因而实多项式的因式分解在不计相伴的意义下（即两个相伴的多项式不认为有区别），是唯一的。

现在把这种思想推广到一类相当广泛的半群中来。

定义 4 设有单位元的可换可消半群 A 的元素 a 有两种分解：

$$a=p_1p_2\cdots p_r,\quad a=q_1q_2\cdots q_s,$$

其中各 p_i 和 q_i 是既约元，若 $r=s$ 且适当排列因子的次序后，p_i 与 q_i 相伴，$i=1,2,\cdots,r$，则称这两种分解为相伴的分解。

定义 5 如果有单位元的可换可消半群 A 的不可逆元都可以分解为有限个既约元的乘积，而且任意两个这种分解是相伴的，则称 A 是唯一分解半群，或称高斯（Gauss）半群注。

注意：如果 A 的元素都是可逆元，也认为是唯一分解

注 K.F.Gauss(1777—1855)德国著名数学家。

半群．另外，定义 5 中的 A 是指有单位元的可换可消半群，其他半群，自然不是唯一分解半群．

由整数和多项式的因子分解性质知，$\langle \boldsymbol{Z}^*, \cdot\rangle$和$\langle \boldsymbol{R}^*[x], \cdot\rangle$都是唯一分解半群．

如整数 24 的两种分解

$$24 = 2\cdot 2\cdot 3\cdot 2 = (-2)\cdot(-3)\cdot 2\cdot 2$$

是相伴的．实多项式 x^4-1 的两种分解

$$\begin{aligned} x^4-1 &= (x^2+1)(x-1)(x+1) \\ &= [2(x^2+1)][-(x+1)]\left[-\frac{1}{2}(x-1)\right] \end{aligned}$$

显然也是相伴的．

再如$\langle \boldsymbol{Q}^+, \cdot\rangle$、$\langle \boldsymbol{Q}^*, \cdot\rangle$、$\langle \boldsymbol{R}^+, \cdot\rangle$、$\langle \boldsymbol{R}^*, \cdot\rangle$、$\langle \boldsymbol{C}^*, \cdot\rangle$各半群的元素都是可逆元，所以它们都是唯一分解半群．

例 1　全体偶数按照数的乘法作成半群$\langle \boldsymbol{E}, \cdot\rangle$，它不是唯一分解半群，因为无单位元．

例 2　设 $A=\{\pm 2^n \mid n=0, 1, 2, \cdots\}\subseteq \boldsymbol{Z}^*$．$A$ 关于乘法封闭，因而$\langle A, \cdot\rangle$是一个可换可消半群，单位元是 $2^0=1$．

可逆元有 $\pm 2^0=\pm 1$．其他元素显然不可逆．

± 2 在 A 中无真因子，故为既约元，其他元素都不是既约元，因当 $n>1$ 时，$\pm 2^n=(\pm 2)\cdot 2^{n-1}$．

任意不可逆元显然可分解为既约元之积：

$$\pm 2^n = \overbrace{(\pm 2)\cdot 2\cdots 2}^{n\text{个}}．\quad (n\geqslant 1)$$

其次，如果又有分解

$$\pm 2^n = p_1p_2\cdots p_m,$$

其中 p_i 都是 $\langle A,\cdot\rangle$ 的既约元，即 2 或 -2. m 显然应等于 n，否则上式将不相等. 所以各 p_i 都与 ± 2 相伴，以上两种分解相伴.

$\langle A,\cdot\rangle$ 是唯一分解半群.

下述例子表明，的确存在不是唯一分解半群的有单位元的可换可消半群：

例 3 设 $A=\{a+b\sqrt{5}i \mid a,b\in \mathbf{Z},\ a,b \text{不全为零}\}$. 求证：(1) $\langle A,\cdot\rangle$ 是有单位元的可换可消半群；(2) $\langle A,\cdot\rangle$ 的可逆元是 ± 1；(3) $\langle A,\cdot\rangle$ 不是唯一分解半群.

证明：(1) $A\subseteq \mathbf{C}^*$，$1\in A$. A 关于乘法封闭. 事实上，

$$(a+b\sqrt{5}i)(c+d\sqrt{5}i)=(ac-5bd)+(ad+bc)\sqrt{5}i.$$

由于 $a+b\sqrt{5}i\neq 0$，$c+d\sqrt{5}i\neq 0$，所以其积也不等于零，故 $ac-5bd$ 和 $ad+bc$ 不全为零，以上乘积属于 A. A 是 $\mathbf{C}^*$ 的子半群，因而可换可消的.

(2) 如果 $a+b\sqrt{5}i$ 是可逆元，则有 $c+d\sqrt{5}i$ 适合 $(a+b\sqrt{5}i)(c+d\sqrt{5}i)=1$. 因而

$$(a^2+5b^2)(c^2+5d^2)=1.$$

所以，必有 $a^2=c^2=1$，$b=d=0$.

这样，A 的可逆元只能是 ± 1. $\alpha\in A$ 的相伴元只有 α 和 $-\alpha$.

(3) $9\in A$. 下面证明 9 有两个不相伴的分解. 易见

$$9=3\cdot 3=(2+\sqrt{5}i)(2-\sqrt{5}i) \tag{1}$$

3 和 $2+\sqrt{5}i$、$2-\sqrt{5}i$ 都是既约元. 事实上，如果 $3=(a+b\sqrt{5}i)(c+d\sqrt{5}i)$，那末，

$$9=(a^2+5b^2)(c^2+5d^2).$$

正整数 a^2+5b^2 和 c^2+5d^2 都是 9 的因数，而 9 的正整

数因子分解只有两种：$9=1\cdot 9=3\cdot 3$. 故 a, b, c, d 只能是方程组

$$\begin{cases}a^2+5b^2=3\\c^2+5d^2=3\end{cases}\quad(2)\ 和\quad\begin{cases}a^2+5b^2=1\\c^2+5d^2=9\end{cases}\quad(3)$$

的整数解. 易见，方程组(2)没有整数解，方程组(3)只有整数解 $a=\pm 1$, $b=0$, $c=\pm 3$, $d=0$. 得 $a+b\sqrt{5}i=\pm 1$（可逆元），$c+d\sqrt{5}i=\pm 3$（3 的相伴元），都是平凡因子，所以 3 是既约元. 同法可证 $2+\sqrt{5}i$ 和 $2-\sqrt{5}i$ 也是既约元. 而 3 和 $2+\sqrt{5}i$ 显然不相伴，因而分解式(1)是 9 的两种不相伴的分解.

总之，$\langle A,\cdot\rangle$ 不是唯一分解半群.

* 五、相伴类构成的半群

由定理 2、4、5 可知 A 的可逆元、既约元以及可约元都不会跨越相伴类的界限，现在我们从相伴类的商集的观点进行分析. 把 A 的相伴类的全体组成的集合记为 $\bar{A}$. 在 $\bar{A}$ 中引进法则 $\circ$：

$$[a]\circ[b]=[ab].\tag{4}$$

即规定 a 和 b 所在的相伴类之积为 ab 所在的相伴类.

引理 1 $\circ$ 是 $\bar{A}$ 的代数运算，即 $\langle\bar{A},\circ\rangle$ 是群胚.

证明：如果 $[a]=[a_1]$, $[b]=[b_1]$，则有 A 的可逆元 ε 和 δ，使 $a_1=a\varepsilon$, $b_1=b\delta$，因而 $a_1b_1=(ab)(\varepsilon\delta)$，即 a_1b_1 与 ab 相伴，$[a_1b_1]=[ab]$.

证毕

定理 6 当 $\langle A,\cdot\rangle$ 是有单位元的可换可消半群时，$\langle\bar{A},\circ\rangle$ 也是有单位元的可换可消半群；当 $\langle A,\cdot\rangle$ 为唯一分解半群时，

$\langle \bar{A}, \circ \rangle$也是唯一分解半群.

证明：(1) $\langle \bar{A}, \circ \rangle$是半群．事实上，任取$[a]$，$[b]$，$[c]$ $\in \bar{A}$，则

$$([a]\circ[b])\circ[c]=[a\circ b]\circ[c]=[(ab)c]=[a(bc)]$$
$$=[a]\circ[bc]=[a]\circ([b]\circ[c]).$$

(2) $\langle \bar{A}, \circ \rangle$的单位元是$[e]=G(A)$．事实上，任取$[a]$ $\in \bar{A}$，则$[e]\circ[a]=[ea]=[a]$．同理$[a]\circ[e]=[a]$.

(3) $\langle \bar{A}, \circ \rangle$是可换的．事实上，任取$[a]$，$[b]\in \bar{A}$，则$[a]\circ[b]=[ab]=[ba]=[b]\circ[a]$.

(4) $\langle \bar{A}, \circ \rangle$是可消的．事实上，如果有$[a]\circ[c]=[b]\circ[c]$，则$[ac]=[bc]$．即有可逆元$\varepsilon\in A$，使$ac=\varepsilon bc$，由于$A$是可消半群，得$a=\varepsilon b$．即$[a]=[b]$．同样可由$[c]\circ[a]=[c]\circ[b]$得$[a]=[b]$.

(5) $\langle \bar{A}, \circ \rangle$的可逆元只有$[e]$．事实上，如果$[a]$是可逆元，则有$[b]\in \bar{A}$，使$[a]\circ[b]=[e]$，即$[ab]=[e]$．那末，必有$\varepsilon\in[e]=G(A)$，使$a(b\varepsilon)=e$．即$b\varepsilon=a^{-1}$，$a$可逆，$a\in[e]$，$[a]=[e]$.

(6) $\langle \bar{A}, \circ \rangle$的既约元是且仅是$[p]$，其中$p$是$A$的任意既约元．事实上，任取$\langle A, \cdot \rangle$的既约元$p$，如果$[p]=[a]\circ[b]=[ab]$，则有可逆元$\varepsilon$，使$p=a(b\varepsilon)$．这样，$a$和$b\varepsilon$都是$p$的平凡因子．如果$a$可逆，则$[a]=[e]$，$[p]=[e]\circ[b]=[b]$．如果$a$是$p$的相伴元，则$[a]=[p]$，$[p]\circ[e]=[p]=[a]\circ[b]$，由消去律，$[p]=[b]$．即$[a]$，$[b]$总是$[p]$的平凡因子．反之，设$[q]$是$\bar{A}$的既约元，$q$显然不是$A$的可逆元，若有$q=ab$，那末$[q]=[a]\circ[b]$，$[a]$、$[b]$中必有一个是$[e]$，另一个是$[q]$，即$a$、$b$中有一个是可逆元，另一个是

q 的相伴元. 这说明 q 是 A 的既约元.

(7) 当 $\langle A, \cdot\rangle$ 是唯一分解半群时，$\langle \bar{A}, \circ\rangle$ 也是. 事实上，任取非可逆元 $[a]\in\bar{A}$，即 a 不是 A 的可逆元，由 A 的唯一分解性质，存在 A 中既约元 $p_1, p_2, \cdots, p_n$，使 $a=p_1p_2\cdots p_n$，因而 $[a]=[p_1]\circ[p_2]\circ\cdots\circ[p_n]$，由 (6)，$[p_1]$，$[p_2]$，…，$[p_n]$ 是 $\bar{A}$ 的既约元，如果又有 $[a]=[q_1]\circ[q_2]\circ\cdots\circ[q_m]=[q_1q_2\cdots q_m]$，即 $a=(\varepsilon q_1)q_2\cdots q_m$，$\varepsilon\in G(A)$. 由 A 的唯一分解性质，得 $m=n$，且适当排列因子次序后，p_1 与 εq_1 相伴，因而 p_1 与 q_1 相伴，p_2 与 q_2 相伴，…，p_n 与 q_n 相伴，即 $[p_i]=[q_i]$，$i=1$，…，n.

证毕

当 A 为唯一分解半群时，可约元的既约元因子允许有相伴的差别，但在 $\bar{A}$ 中，除了次序外，因子没有任何不确定性. 如在 $\boldsymbol{R}^*[x]$ 中，

$$
\begin{aligned}
x^2-1&=(x+1)(x-1)\\
&=\left(-\frac{1}{2}x-\frac{1}{2}\right)(-2x+2)\\
&=(2\sqrt{2}x+2\sqrt{2})\left(\frac{x}{2\sqrt{2}}-\frac{1}{2\sqrt{2}}\right)\\
&=\cdots,
\end{aligned}
$$

但在商集的半群中，上述各种相伴的分解只对应一个分解式：

$$[x^2-1]=[x+1]\circ[x-1].$$

习 题 2·3

1. 求证：可换可消半群的子半群也是可换可消半群。

2. 下列半群哪些是可换可消半群：

(1) $\langle \boldsymbol{Z}, \cdot \rangle$；　　(2) $\langle \boldsymbol{R}, + \rangle$；

(3) $\langle M_n(\boldsymbol{R}), \cdot \rangle$；　　(4) $\langle$全体奇数$, \cdot \rangle$。

3. 下列元素在对应半群中是可逆元、既约元还是可约元？

(1) $7 \in \langle \boldsymbol{Z}^*, \cdot \rangle$；　　(2) $4 \in \langle \boldsymbol{Z}^*[x], \cdot \rangle$；

(3) $-20 \in \langle \boldsymbol{Z}^*, \cdot \rangle$；　　(4) $4 \in \langle \boldsymbol{R}^*[x], \cdot \rangle$；

(5) $2x^2+1 \in \langle \boldsymbol{R}^*[x], \cdot \rangle$；　　(6) $4 \in \langle \boldsymbol{Z}^*, \cdot \rangle$；

(7) $x^2-2 \in \langle \boldsymbol{R}^*[x], \cdot \rangle$；　　(8) $4 \in \langle \boldsymbol{R}^*, \cdot \rangle$。

4. 设 $A = \left\{ \frac{3^m}{2^n} \middle| m, n \in \boldsymbol{N} \right\}$.

(1) 求证：$\langle A, \cdot \rangle$是有单位元的可换可消半群；

(2) 写出A的所有可逆元；

(3) 写出A的所有既约元；

(4) 将$\frac{3^2}{2^3}$分解成既约元的乘积；

(5) $\langle A, \cdot \rangle$是否唯一分解半群？为什么？

5. 设 $\boldsymbol{Z}^*[i] = \{a+bi \mid a, b \in \boldsymbol{Z},\ a, b$ 不全为零$\}$. 求证：$\langle \boldsymbol{Z}^*[i], \cdot \rangle$是有单位元的可换可消半群；可逆元是且仅是 1, -1, i, $-i$；$1+2i$ 是既约元。

6. 在$\langle \boldsymbol{N}, + \rangle$中，求证：

(1) a 整除 b 当且仅当 $a \leqslant b$；

(2) 既约元只有 1，可逆元只有 0；

(3) 它是唯一分解半群.

7. 例 3 的半群中，求证 $2+\sqrt{5}i$ 不整除 3 .

*8. 设W是分母与 10 互素非零既约分数的集合. 求证：W关于乘法作成有单位元的可换可消半群；其可逆元形如$\frac{a}{b}$，a，b，都与 10 互素；其既约元形如$\frac{a}{b}$，b 与 10 互素，a 有一个单因数 2 或 5 ；W是唯一分解半群.

§ 2·4 同态与同构

集合的映射本身并不涉及集合的代数运算，如果两个群胚之间有一个映射，考虑映射与群胚乘法的关系，就显得复杂一些. 一般说来，映射与两个群胚的乘法不见得一致，就是说，两元素之积的象不一定正好等于这两元素象之积. 比如规定$\langle \mathbf{C}, \cdot\rangle$到$\langle \mathbf{R}, \cdot\rangle$的映射 φ 为：

$$\varphi(a)=\operatorname{Re} a,$$

其中 Re 表示 a 的实部. 这时

$\varphi(ab)=\operatorname{Re}(ab)$和 $\varphi(a)\varphi(b)=\operatorname{Re} a\cdot\operatorname{Re} b$ 一般是不相等的，如 $\varphi(i\,i)=\operatorname{Re} i^2=-1$，而 $\varphi(i)\varphi(i)=0\cdot 0=0$.

与群胚乘法保持一致的映射是特别重要的，这一节专门讨论这种映射.

一、同态的概念

定义 1 设$\langle A, \cdot\rangle$和$\langle \bar{A}, *\rangle$是两个群胚，$\varphi$ 是 A 到 $\bar{A}$ 的映射，如果对任意的 a，$b\in A$，都有

$$\varphi(a\cdot b)=\varphi(a)*\varphi(b), \tag{1}$$

则称 φ 是 $\langle A,\cdot\rangle$ 到 $\langle \bar{A},*\rangle$ 的同态映射，简称同态。满射的同态称为满同态，单射的同态称为单同态。如果 A 中的变换是同态映射，则称为自同态变换，简称自同态。如果存在 $\langle A,\cdot\rangle$ 到 $\langle \bar{A},*\rangle$ 的满同态，则称 $\langle A,\cdot\rangle$ 与 $\langle \bar{A},*\rangle$ 同态。

例 1 设 $\boldsymbol{R}$ 到 $\boldsymbol{R}$ 的映射 φ 如下：

$$\varphi(a)=10^a.$$

求证：φ 是 $\langle \boldsymbol{R},+\rangle$ 到 $\langle \boldsymbol{R},\cdot\rangle$ 的同态。

证明：任取 $a,b\in\boldsymbol{R}$，则

$$\varphi(a+b)=10^{a+b}=10^a\cdot 10^b=\varphi(a)\cdot\varphi(b),$$

故 φ 是同态。易见 φ 是单同态，不是满同态。

注意：不能说 φ 是自同态，因为 $\langle \boldsymbol{R},+\rangle$ 和 $\langle \boldsymbol{R},\cdot\rangle$ 是不同的两个半群。

例 2 用 $M_2(\boldsymbol{R})$ 表示实二阶方阵的集合。设有 $M_2(\boldsymbol{R})$ 到 $\boldsymbol{R}$ 的映射如下：

$\varphi_1(T)=|T|$；（方阵 T 的行列式）

$\varphi_2(T)=a_{11}$；（T 的左上角元素）

$\varphi_3(T)=1$。

试问：φ_1，φ_2，φ_3 是不是 $\langle M_2(\boldsymbol{R}),\cdot\rangle$ 到 $\langle \boldsymbol{R},\cdot\rangle$ 的同态？

解：任取 T，$S\in M_2(\boldsymbol{R})$，则

$$|T\cdot S|=|T|\cdot|S|.$$

也即 $\varphi_1(T\cdot S)=\varphi_1(T)\cdot\varphi_1(S)$，说明 φ_1 是同态，且显然是满同态，不是单同态，因不同矩阵的行列式可以相同。

设 $T=(a_{ij})$，$S=(b_{ij})$，则 TS 第 i 行第 j 列的元素是 $a_{i1}b_{1j}+a_{i2}b_{2j}$。特别，$TS$ 左上角的元素应是 $a_{11}b_{11}+a_{12}b_{21}$，即

$$\varphi_2(TS)=a_{11}b_{11}+a_{12}b_{21}.$$

而 $\varphi_2(T)\cdot\varphi_2(S)=a_{11}b_{11}$，一般不等于 $\varphi_2(TS)$。如取 $T=\begin{pmatrix}1 & 1\\0 & 0\end{pmatrix}$，$S=\begin{pmatrix}1 & 0\\1 & 0\end{pmatrix}$，则 $TS=\begin{pmatrix}2 & 0\\0 & 0\end{pmatrix}$，即 $\varphi_2(TS)=2$，但 $\varphi_2(T)=1=\varphi_2(S)$，故 $\varphi_2(TS)\neq\varphi_2(T)\cdot\varphi_2(S)$，$\varphi_2$ 不是同态。

$$\varphi_3(ST)=1=1\cdot1=\varphi_3(S)\cdot\varphi_3(T),$$

φ_3 是同态。φ_3 既非满同态又非单同态。

例 3 找出 $\langle \mathbf{Z},+\rangle$ 的所有自同态。

解： 设 φ 是一个自同态，任取 $a\in\mathbf{Z}$，由于 $0+a=a$，故

$$\varphi(a)=\varphi(0+a)=\varphi(0)+\varphi(a).$$

所以 $\varphi(0)=0$，即 0 的象还是 0。

而 $0=\varphi(0)=\varphi(a-a)=\varphi(a)+\varphi(-a)$，故有 $\varphi(-a)=-\varphi(a)$。令 $\varphi(1)=p$，设 n 是任意正整数，则 $\varphi(n)=\varphi(1+1+\cdots+1)=\varphi(1)+\varphi(1)+\cdots+\varphi(1)=pn$。

$$\begin{aligned}\varphi(-n)&=\varphi(-1-1-\cdots-1)\\&=\varphi(-1)+\varphi(-1)+\cdots+\varphi(-1)\\&=-p-p-\cdots-p=-np.\end{aligned}$$

由此可见，自同态应形如

$$\varphi(a)=pa, \tag{1}$$

其中 p 是一个固定的整数。

反之，任意取定整数 p，规定变换 φ 如 (1) 所示，则易见 φ 是自同态。所以自同态有无穷多个。

二、同态的性质

如果群胚 $\langle A,\cdot\rangle$ 与 $\langle \bar{A},*\rangle$ 同态，则 A 的某些性质可以转移到 $\bar{A}$ 中来。

定理1 设群胚$\langle A,\cdot\rangle$与群胚$\langle\bar{A},*\rangle$同态，同态映射设为σ，则

(1) 如果A是半群，则$\bar{A}$也是半群；

(2) 如果A是可换半群，则$\bar{A}$也是可换半群；

(3) 如果半群A在单位元e，则$\sigma(e)$是$\bar{A}$的单位元；

(4) 如果半群A有零元0，则$\sigma(0)$是$\bar{A}$的零元；

(5) 如果a是半群A的可逆元，则$\sigma(a)$也是$\bar{A}$的可逆元，且$\sigma(a^{-1})$是其逆元.

证明：以(1)、(3)为例，其余请读者完成.

(1) 任取$\bar{a}$，$\bar{b}$，$\bar{c}\in\bar{A}$，由于σ是满同态，必有a，b，$c\in A$，使$\sigma(a)=\bar{a}$，$\sigma(b)=\bar{b}$，$\sigma(c)=\bar{c}$。而

$$\begin{aligned}\sigma((ab)c)&=\sigma(ab)*\sigma(c)=(\sigma(a)*\sigma(b))*\sigma(c)\\&=(\bar{a}*\bar{b})*\bar{c},\\ \sigma(a(bc))&=\sigma(a)*\sigma(bc)=\sigma(a)*(\sigma(b)*\sigma(c))\\&=\bar{a}*(\bar{b}*\bar{c}).\end{aligned}$$

由A是半群，适合结合律，因而$(ab)c=a(bc)$，故以上两式右端相等，即$\bar{A}$是半群.

(3) 任取$\bar{a}\in\bar{A}$，则有$a\in A$，使$\sigma(a)=\bar{a}$，$\sigma(e)*\bar{a}=\sigma(e)*\sigma(a)=\sigma(ea)=\sigma(a)=\bar{a}$，同理$\bar{a}*\sigma(e)=\bar{a}$。即$\sigma(e)$是$\bar{A}$的单位元.

证毕

三、特殊的同态——同构

同态的群胚有许多共同的性质，但仍可能有很大差别. 如从例2可见，φ_3是$\langle M_2(R),\cdot\rangle$到$\langle\{1\},\cdot\rangle$的满同态. 但前者是不可换的，后者可换，前者含无穷多个元素，后者是单

元素集．此外，一般说来，还有一些性质，如无单位元、无零元等也不能通过同态转移到同态象集中去．之所以如此，是因为同态满射不一定是一一映射．下面引进一种特殊的同态——同构，可以克服这一缺点．

定义 2 群胚 A 到群胚 $\bar{A}$ 的同态如果又是一一映射，则称为同构映射，简称同构．如果 A 到 $\bar{A}$ 的同构映射存在，则称 A 与 $\bar{A}$ 同构，记为 $A\cong\bar{A}$．A 到自身的同构映射，称为自同构变换，简称自同构．

同态不具有对称性，如 A 与 $\bar{A}$ 同态，不一定 $\bar{A}$ 与 A 同态．但同构有对称性，如果 A 与 $\bar{A}$ 同构，则必然 $\bar{A}$ 与 A 同构，因为同构映射是一一映射，其逆映射显然是 $\bar{A}$ 到 A 的同构[注]．同构的群胚除等势外，还具有性质完全相同的代数运算．它们同时是或不是半群；运算同时是可换的或不可换的；单位元、零元、逆元同时存在或不存在，且相互对应；具有相同的乘法表；等等．总之，它们除符号和名称不同外，本质是完全一样的．因而掌握了一个群胚就等于掌握了与它同构的一类群胚，这对于讨论具体群胚带来极大方便．

例 4 求证：$\langle \boldsymbol{R}, +\rangle\cong\langle \boldsymbol{R}^{+}, \cdot\rangle$．

证明：由例 1，$\varphi(a)=10^{a}$ 是同态．显然 φ 是 $\boldsymbol{R}$ 到 $\boldsymbol{R}^{+}$ 的一一映射，因而是同构．

例 5 §2·2 五中提到的半群有哪些自同构？

解：设 σ 是 A 的自同构，A 的单位元是 d，零元是 c，所以由定理 1，$\sigma(d)=d,\sigma(c)=c$。如果 $\sigma_1(a)=a$，由于 σ_1 是单

注　这一点可以证明如下：设 φ 是 A 到 $\bar{A}$ 的同构，任取 $\bar{a}$，$\bar{b}\in\bar{A}$，$\varphi^{-1}(\bar{a})=a,\varphi^{-1}(\bar{b})=b$，则 $\varphi^{-1}(\bar{a}*\bar{b})=\varphi^{-1}(\varphi(a)*\varphi(b))=\varphi^{-1}(\varphi(ab))=ab=\varphi^{-1}(\bar{a})\varphi^{-1}(\bar{b})$．

射，$\sigma_1(b)$只能为b．这时 $\sigma_1=\varepsilon_A$，自然是自同构．如果 $\sigma_2(a)=b$，则 $\sigma_2(b)=a$．下面证明 σ_2 是同态．事实上，由于 $\sigma_2(d)=d$ 是单位元，$\sigma_2(c)=c$ 是零元，而运算是可换的，只须验证：$\sigma_2(a\cdot a)=\sigma_2(a)\cdot\sigma_2(a)$，$\sigma_2(a\cdot b)=\sigma_2(a)\cdot\sigma_2(b)$，$\sigma_2(b\cdot b)=\sigma_2(b)\cdot\sigma_2(b)$．由运算表，不难证明它们都是成立的．$\sigma_2$ 显然是一一映射，故是自同构．总之，A 的自同构只有 σ_1,σ_2．

例 6　判断是否$\langle \boldsymbol{R},\cdot\rangle\cong\langle \boldsymbol{R},+\rangle$？

解：如果同构，应同时有或无零元，前者有零元——数0，而后者无零元（见§2·2 三），故不同构．

另解：如果同构，设 σ 是一个同构映射，则 σ^{-1} 是后者到前者的同构．假定 $\sigma(-1)=a$，$\sigma^{-1}\left(\frac{a}{2}\right)=p$，那末 $p^2=pp=\sigma^{-1}\left(\frac{a}{2}\right)\cdot\sigma^{-1}\left(\frac{a}{2}\right)=\sigma^{-1}\left(\frac{a}{2}+\frac{a}{2}\right)=\sigma^{-1}(a)=-1$，即实数 $p=\pm i$，这不可能．

习　题　2·4

1．设半群 A 与 $\bar{A}$ 同态，同态为 σ．

(1) 求证：如果 $a|b$，则$\sigma(a)|\sigma(b)$；如果 a 与 b 相伴，则 $\sigma(a)$与 $\sigma(b)$相伴．

(2) 试问：既约元的象是否既约元？可约元的象是否可约元？若 A 是可消半群，那末 $\bar{A}$ 是否可消半群？

2．求证：$\langle \boldsymbol{Z},+\rangle$与全体奇数作成的加半群$\langle \boldsymbol{D},+\rangle$不同态，与全体奇数作成的乘半群$\langle \boldsymbol{D},\cdot\rangle$也不同态．

3．求证：有限半群的自同态满射也是自同构．

4．设 $M=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\middle| x\in \boldsymbol{R}\right\}$．求证：$\langle M,\cdot\rangle\cong\langle \boldsymbol{R},+\rangle$．

5. 设 $A=\{a\in\mathbf{Q}\mid a>1\}$，$B=\{b\in\mathbf{Q}\mid 0<b<1\}$. 求证：$\langle A,\cdot\rangle\cong\langle B,\cdot\rangle$.

6. 设 φ 是 $\boldsymbol{P}$ 到 $A=\{0,\ 1\}$ 的映射：$\varphi(1)=1$，$\varphi(n)=0(n>1)$. 求证：φ 是 $\langle \boldsymbol{P},\cdot\rangle$ 到 $\langle A,\cdot\rangle$ 的同态.

7. 以下映射是否 $\langle \mathbf{Z}^*,\cdot\rangle$ 的自同态？

(1) $\varphi_1(a)=|a|$；　　(2) $\varphi_2(a)=2a$；

(3) $\varphi_3(a)=a^2$；　　(4) $\varphi_4(a)=-a$.

8. 找出 $\langle \mathbf{Z},+\rangle$ 的所有自同构.

9. 求证：$\{a+b\sqrt{3}\mid a,\ b\in\mathbf{Z}\}$ 与 $\{a+b\sqrt[3]{3}\mid a,b\in\mathbf{Z}\}$ 关于加法作成的半群同构，关于乘法作成的半群不同构.

10. 设 $\langle A,\cdot\rangle$ 是可换半群，A^* 是其可逆元集合，$B=\{0,1\}$，$\varphi(a)=\begin{cases}1, a\in A^*;\\ 0, a\in A\backslash A^*.\end{cases}$ 求证：φ 是 $\langle A,\cdot\rangle$ 到 $\langle B,\cdot\rangle$ 的同态.

本 章 提 要

一、群胚：具有一个代数运算的集合.

二、半群：适合结合律的群胚.

三、a 整除 b：存在 c，d，使 $ac=b$，$da=b$.

四、单位元 e：对任意元素 a，有 $ae=ea=a$.

五、零元 0：对任意元素 a，有 $a0=0a=0$.

六、可逆元 a：存在 a^{-1}，使 $aa^{-1}=a^{-1}a=e$.

七、唯一分解半群：有单位元的可换可消半群，其不可逆元可分解为有限个既约元之积，且分解相伴唯一.

八、群胚的同态与同构：群胚到群胚的保持运算的映射，称为群胚同态. 一一映射的同态称为同构.

复 习 题 二

1．以下群胚的乘法是否适合结合律或交换律？

（1） $\mathbf{Z}$ 中规定 $a*b=a-b$；

（2） $\mathbf{Q}$ 中规定 $a*b=ab+1$；

（3） $\mathbf{Q}$ 中规定 $a*b=\frac{1}{2}ab$；

（4） $\boldsymbol{P}$ 中规定 $a*b=2^{ab}$；

（5） $\boldsymbol{P}$ 中规定 $a*b=a^b$．

*2．设 $|A|=n$，那末 A 中可以规定多少种不同的可换的代数运算？

*3．在 $\langle M_n(\mathbf{R}),\cdot\rangle$ 中，求证：B 是 A 的右因子当且仅当 $\begin{pmatrix}A\\B\end{pmatrix}$ 的秩 $=B$ 的秩．B 是 A 的左因子当且仅当 (AB) 的秩 $=B$ 的秩．

*4．设半群 A 有右单位元 e，A 的每个元素是 e 的左因子，求证 A 的元素都可逆．

5．下列群胚是否半群？有否单位元或零元：

（1） $\langle\mathbf{R},*\rangle$，其中 $a*b=\sqrt{a^2+b^2}$（算术根）；

（2） $\langle\mathbf{Z},\circ\rangle$，其中 $a\circ b=\mathrm{Max}\{a,\ b\}$；

（3） $\langle\mathbf{Z},☆\rangle$，其中 $a☆b=a+b+ab$；

（4） $\langle S,\circ\rangle$，其中 $a\circ b=(a,b)$，$S=\{1,2,3,4,5,6,7\}$；

（5） $\langle T,*\rangle$，其中 $a*b=[a,b]$，$T=\{1,2,4,5,10,20\}$．

6．在 $\mathbf{R}$ 中，p，q，r 是固定的数，规定 $a\circ b=pa+qb+r$．说明何时这个代数运算适合交换律、结合律或消去律？

7．设 A 为群胚，B、C 是 A 的子集，定义 $BC=\{bc|b$

$\in B$，$c\in C\}$为 B 与 C 的积集。

在$\langle \mathbf{Q},\cdot\rangle$中求 $\mathbf{QQ}$，$\mathbf{QZ}$，$\mathbf{ZQ}$，$\mathbf{ZZ}$，$\mathbf{Q}^+\mathbf{Q}^+$。

8．设群胚 A 的乘法表为：

	a	b	c
a	a	a	a
b	a	a	a
c	b	b	b

求$(AA)A$ 和 $A(AA)$。

9．设 K_1，K_2，K_3，K_1'，K_2' 是群胚 A 的子集，且$K_1'\subseteq K_1$，$K_2'\subseteq K_2$，求证：

（1）$K_1(K_2\cup K_3)=K_1K_2\cup K_1K_3$；

（2）$K_1(K_2\cap K_3)\subseteq K_1K_2\cap K_1K_3$；

（3）$K_1'K_2'\subseteq K_1K_2$。

10．设 $\mathbf{C}^*[x]$是所有非零复多项式组成的集合.以下 φ_i 都是$\mathbf{C}^*[x]$到 $\mathbf{C}$ 的映射，试问哪些是$\langle \mathbf{C}^*[x],\cdot\rangle$到$\langle \mathbf{C},\cdot\rangle$的同态？

设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n(a_0\neq 0)$。

（1）$\varphi_1(f)=a_0$；　　（2）$\varphi_2(f)=\bar{a}_0$；

（3）$\varphi_3(f)=a_0+a_1+\cdots+a_n$；　　（4）$\varphi_4(f)=a_0+a_n$；

（5）$\varphi_5(f)=|a_n|$；　　（6）$\varphi_6(f)=2^n$；

（7）$\varphi_6(f)=1$。

11．在半群中，如果 $a^2=a$，则称 a 为幂等元．求证：可换半群的全体幂等元作成子半群．

12．设 A 是有单位元的可换可消半群，$\bar{A}$ 是其全体相伴类集合，求证：$\langle A,\cdot\rangle$与$\langle \bar{A},\circ\rangle$同态(见§2·3 五)。

13 设 $\mathbf{D}^+$是全体正奇数的集合.求证：$\langle \mathbf{D}^+,\cdot\rangle$ 是唯一分解半群．其可逆元有哪些？既约元有哪些？

*14．设半群 A 中任意两个不同元素不可换，求证 A 的每个元素都是幂等元．半群具有以上性质的充要条件是：对于任意两个元素 x,y，成立 $xyx=x$，$yxy=y$。

第三章　群

群论是近世代数的主要内容之一，也是学习环、域等内容必不可少的准备.

本章将介绍群论中的基本概念和定理，同时还讨论一些具体的群.

§3·1　什么是群？

本节由半群引出群的概念，进而介绍群的几个等价定义.

在一个有单位元的半群里，单位元是一个可逆元，还可能有其他可逆元. 如果半群的所有元素都可逆，那末这种半群就有特殊的意义.

定义1　有单位元的半群$\langle G,\cdot\rangle$，如果每个元素都是可逆元，则称为群.

由§2·3定理3，一个元素可逆当且仅当它是单位元的因子. 这样，又有

定义2　有单位元的半群$\langle G,\cdot\rangle$中每个元素如果都是单位元的因子，则称为群.

抛开半群的概念，群也可以直接写成

定义3　设G是非空集合，且

（1）G中有一个代数运算·，称为乘法；

(2) G 关于 · 适合结合律；

(3) G 中存在元素 e，对于任意 $g\in G$，有 $eg=ge=g$；

(4) 对 G 中每个元素 g，可以找到 $g^{-1}\in G$，使 $g^{-1}g=gg^{-1}=e$。

这时，称 $\langle G,\cdot\rangle$ 为群。

定义 3 中，(1)说明 $\langle G,\cdot\rangle$ 是群胚，(1)、(2)说明它是半群，(3)说明有单位元，(4)说明每个元素可逆。实质上就是定义 1 的另一种说法。

以上三个定义从不同方面反映了群的两个最本质的特点：第一，群中有适合结合律的代数运算；第二，这个代数运算有逆运算。

我们在判断一个代数系是不是群时，用任何一个定义都是允许的，不熟悉半群的读者，可以使用定义 3 。

例 1　$\langle \mathbf{Z},+\rangle$ 是群，而 $\langle \mathbf{Z},\cdot\rangle$ 不是群.

事实上，$\langle \mathbf{Z},+\rangle$ 是半群，单位元是 0 ，任意元素 a 的逆元是 $-a$，由定义 1 ，$\langle \mathbf{Z},+\rangle$ 是群. $\langle \mathbf{Z},\cdot\rangle$ 虽是半群，且有单位元，但某些元素(如 2)没有逆元. 所以 $\langle \mathbf{Z},\cdot\rangle$ 不是群.

例 2　$\langle \mathbf{Q}^*,\cdot\rangle$ 是群，但 $\langle \mathbf{Q},\cdot\rangle$ 不是群.

事实上，半群 $\langle \mathbf{Q}^*,\cdot\rangle$ 的单位元是 1 ，任取 $a\in \mathbf{Q}^*$，$\frac{1}{a}$ 也在 $\mathbf{Q}^*$ 中，$a\cdot\frac{1}{a}=\frac{1}{a}\cdot a=1$，故 a 是 1 的因子. 由定义 2 ，$\langle \mathbf{Q}^*,\cdot\rangle$ 是群.

$\langle \mathbf{Q},\cdot\rangle$ 虽是有单位元 1 的半群，但 $0\in \mathbf{Q}$ 显然不是 1 的因子，所以 $\langle \mathbf{Q},\cdot\rangle$ 不是群.

例 3　设 $U_n=\{\varepsilon_0,\varepsilon_1,\cdots,\varepsilon_{n-1}\}$，其中

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, k=0,1,\cdots,n-1,$$

是 n 次单位根. 求证 U_n 关于乘法成群.

$\langle U_n,\cdot\rangle$ 常称为 n 次单位根乘群.

证明: 任取 ε_i, $\varepsilon_j \in U_n$, 则

$$(\varepsilon_i\varepsilon_j)^n = \varepsilon_i^n\varepsilon_j^n = 1\cdot 1 = 1.$$

即 $\varepsilon_i\varepsilon_j \in U_n$, U_n 关于乘法封闭. 另外, 结合律显然成立. 所以 $\langle U_n,\cdot\rangle$ 是半群, $\varepsilon_0 = 1$ 是单位元. 而且 $\frac{1}{\varepsilon_i}$ 也是 n 次单位根, 这因为

$$\left(\frac{1}{\varepsilon_i}\right)^n = \frac{1}{\varepsilon_i^n} = 1.$$

故 U_n 的元素都可逆, 即 $\langle U_n,\cdot\rangle$ 是群.

例 4 设 $B_4 = \{a,b,c,d\}$. B_4 中规定乘法如表所示.

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

容易验证, 乘法适合结合律, 所以 $\langle B_4,\cdot\rangle$ 是半群.

表中第一行与第一列的元素依次都是 a, b, c, d, 所以 a 是单位元(见§2·2 五). 同时, 每一行及每一列中都有 a 出现, 说明每个元素都是 a 的因子. 由定义 2, $\langle B_4,\cdot\rangle$ 是群. 称为克莱茵(Klein)四元群[注].

例 5 集合 $\boldsymbol{R}^*\times\boldsymbol{R}$ 中规定

$$(a,b)\cdot(c,d) = (ac, bc+d). \qquad (1)$$

求证 $\langle \boldsymbol{R}^*\times\boldsymbol{R},\cdot\rangle$ 是群.

注 F·Klein(1849—1925), 德国数学家.

证明：(1)式是代数运算．下面证结合律．由(1)式，

$$
\begin{aligned}
&((a,b)\cdot(c,d))\cdot(h,k)\\
=&(ac,bc+d)\cdot(h,k)\\
=&(ach,bch+dh+k);\\
&(a,b)\cdot((c,d)\cdot(h,k))\\
=&(a,b)\cdot(ch,dh+k)\\
=&(ach,bch+dh+k).
\end{aligned}
$$

(1,0)是单位元．事实上，由(1)，

$$
\begin{aligned}
&(a,b)\cdot(1,0)\\
=&(a\cdot 1,b\cdot 1+0)\\
=&(a,b),\\
&(1,0)\cdot(a,b)\\
=&(1\cdot a,0\cdot a+b)\\
=&(a,b).
\end{aligned}
$$

(a,b)的逆元是$\left(\frac{1}{a},-\frac{b}{a}\right)$．事实上，

$$
\begin{aligned}
(a,b)\cdot\left(\frac{1}{a},-\frac{b}{a}\right)&=\left(a\cdot\frac{1}{a},b\cdot\frac{1}{a}-\frac{b}{a}\right)\\
&=(1,0).\\
\left(\frac{1}{a},-\frac{b}{a}\right)\cdot(a,b)&=\left(\frac{1}{a}\cdot a,-\frac{b}{a}\cdot a+b\right)\\
&=(1,0).
\end{aligned}
$$

根据定义 3，$\langle \boldsymbol{R}^*\times\boldsymbol{R},\cdot\rangle$是群．

例 6 用 $M_n^*(\boldsymbol{R})$表示非退化实 n 阶方阵的集合．显然它关于矩阵乘法作成群．其单位元是单位方阵，元素的逆元是对应的逆方阵．

最简单的群，要算单位元群了：

例 7 设单元素集$\{e\}$中有乘法运算$e\cdot e=e$，则$\langle\{e\},\cdot\rangle$显然是群，$e$是这个群的单位元。常称之为单位元群。

例 8 以n为模的剩余类$\mathbf{Z}_n$关于剩余类加法作成半群（§2·1 例 7）。$[0]$是单位元，这因为$[a]+[0]=[0]+[a]=[a+0]=[a]$。$[a]$的逆元是$[-a]$，这因为$[-a]+[a]=[a]+[-a]=[0]$。由定义 3，$\langle\mathbf{Z}^n,+\rangle$作成群。

注意：$\langle\mathbf{Z}_n,\cdot\rangle(n>1)$不是群，事实上，$[1]$虽是单位元，但$[0]\in\mathbf{Z}_n$却无逆元。

习 题 3·1

1．在$\mathbf{Q}^+$中定义$a\circ b=\frac{1}{2}ab$，求证$\langle\mathbf{Q}^+,\circ\rangle$是群。其单位元是什么？元素$a$的逆元是什么？

2．设$S=\mathbf{R}\setminus\{-1\}$，规定$a*b=a+b+ab$，求证：$\langle S,*\rangle$是群。在$S$中找出适合$2*x*3=7$的元素。

3．设$\langle G,\cdot\rangle$是群，若在G中规定$a*b=b\cdot a$，求证$\langle G,*\rangle$也是群。

4．以下哪些是群？

(1) $\langle M^*(\mathbf{R}),+\rangle$；

(2) $\langle\{z\in\mathbf{C}\mid|z|=1\},\cdot\rangle$；

(3) $\left\langle\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix}\right\},\cdot\right\rangle$；

*(4) $\langle\mathbf{R}^*,\circ\rangle$，　$x\circ y=\begin{cases}xy,&(x>0),\\x/y,&(x<0)；\end{cases}$

(5) $\left\langle\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,b\in \mathbf{R}, a^2+b^2\neq 0\right\}, \cdot\right\rangle$.

§3·2 群的基本性质

一、从半群到群

群既然是半群，所以半群的性质群都具备. 由半群的单位元和逆元的性质，可得

定理 1 群的单位元是唯一的，每个元素的逆元也是唯一的.

另外，由§2·2定理4，可得

定理 2 群的任意两个元素互相整除.

此定理的逆命题也成立. 由此可得群的重要判别定理：

定理 3 半群$\langle G,\cdot\rangle$是群的充要条件是G的任意两个元素互相整除.

证明：必要性即定理2. 下面证充分性.

任取$a\in G$. 由于a是a的因子，故存在e和$e'\in G$，使

$$ea=a, \quad ae'=a.$$

任取$b\in G$，由于b是a的因子，故存在c和$c'\in G$，使

$$ac=b, \quad c'a=b.$$

因而$eb=e(ac)=(ea)c=ac=b$.

所以，e是左单位元.

另一方面，$be'=(c'a)e'=c'(ae')=c'a=b$.

所以，e'是右单位元。

半群$\langle G,\cdot\rangle$中同时存在左、右单位元，由§2·2 定理 1，$e=e'$ 是单位元。

既然G的任意元素整除所有元素，自然也整除单位元 e。由上节定义 2，$\langle G,\cdot\rangle$是群。

证毕

两个元素互相整除，就是对任意的 a，b，方程 $ax=b$ 和 $ya=b$ 总有解。因而定理 3 可以改写成。

定理 4 半群 $\langle G,\cdot\rangle$ 是群的充要条件是：对于任意的 $a,b\in G$，方程 $ax=b$，$ya=b$ 在G中有解。

定理 4 常作为群的定义。

我们知道，半群有零元的概念，那末，群中有没有零元呢？

定理 5 除了单位元群外，所有群都没有零元。

证明由§2·2 定理 5 得到。

注意：单位元群$\langle\{e\},\cdot\rangle$中 e 是单位元，也可看作零元，同时 e 还是本身的逆元。

在带有单位元的半群A里，全体可逆元构成一个子半群$G(A)$（§2·2 定理 7）。不仅如此，由于可逆元存在逆元，其逆元也可逆，又得

定理 6 有单位元的半群A中全体可逆元构成群$G(A)$。

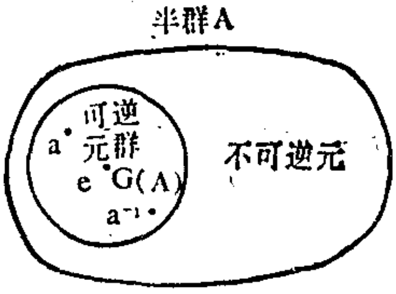


图 3—1

这个群称为半群的可逆元群。这是半群中包含的最大群，因为半群的其他元素都无逆元，自然不可能成为群的元素。（如图 3—1）

当这个半群是群时，可逆元群正好充满整个半群。这时，不难证

明：

定理7 在群$\langle G,\cdot\rangle$中，

(1) $(a^{-1})^{-1}=a$；

(2) $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$；

(3) $(a^t)^{-1}=(a^{-1})^t$（t 为正整数）。

（(3)是(2)的特例）

二、群的类型

前面的许多例子，虽然是群，但又千差万别，为了细致深入地研究群，必须根据不同的特点将群分为不同的类型。

如依照群中所含元素的多少可分成有限群与无限群。群里只有有限个元素时，称为有限群，否则称为无限群。有限群G所含元素的个数$|G|$，称为群G的阶。上节例1、例2、例5、例6都是无限群，其他四个例子都是有限群，例3中$|U_n|=n$，例4中$|G|=4$，例7中则是1阶群，例8中$|\mathbf{Z}_n|=n$。例3说明，对于任意的自然数n，总有n阶群。

依照群中的乘法是否可换，群又分为可换群与不可换群。上节例1、例2、例3、例4、例7、例8都是可换群，而例5和例6则是不可换群。事实上，例5中有

$$
\begin{aligned}
&(1,1)(0,1)\\
&=(1\cdot 0,1\cdot 0+1)\\
&=(0,1),\\
&(0,1)(1,1)\\
&=(0\cdot 1,1\cdot 1+1)\\
&=(0,2).
\end{aligned}
$$

而例6的矩阵乘法的不可换性早已熟知。

可换群也称为阿贝耳(Abel)群[注]，其代数运算常称为加法，记为+。这时，群叫做加群。今后凡提到加群，都理解为可换群。加群中，单位元记为0，称为零元(不要与半群中的零元相混)，而a的逆元，称为a的负元，记为$-a$。

三、元素的方幂

半群中元素的正整数方幂a^n规定为n个a的乘积，这种记号在群中仍然适用。此外，半群的可逆元a的逆元记为a^{-1}，它不仅是一个记号，也作为一个规定：a的负1次方幂规定为a的逆元。此外，a的负整数次方幂a^{-n}，规定为a的逆元的n次方幂$(a^{-1})^n$。群的元素都可逆，所以以上记号适用于群的所有元素。至于群中每个元素的零次方幂，将规定为单位元e。总之，

$$a^n=\begin{cases}aa\cdots a, & (n>0);\\ e, & (n=0);\\ (a^{-1})(a^{-1})\cdots(a^{-1}), & (n<0).\end{cases}\tag{1}$$

在加群中，a的n次方幂记为na。因而

$$na=\begin{cases}a+a+\cdots+a, & (n>0);\\ 0, & (n=0);\\ (-a)+(-a)+\cdots+(-a), & (n<0);\end{cases}\tag{2}$$

定理8 群中通常的指数法则成立：

$$a^m a^n=a^{m+n};\tag{3}$$

$$(a^m)^n=a^{mn},\tag{4}$$

其中m，n为任意整数。

注 N. H. Abel(1802—1829)，挪威青年数学家。

证明留给读者。

对于加群，(3)，(4)式变为

$$ma+na=(m+n)a; \tag{5}$$

$$m(na)=mna. \tag{6}$$

此外，由于运算可换，可得

$$ma+mb=m(a+b), \tag{7}$$

其中 m，n 为任意整数。

四、消去律

群是可消半群，因为由 $ax=bx$，得 $axx^{-1}=bxx^{-1}$，即 $a=b$。同理，由 $xa=xb$，得 $a=b$。

可消半群不一定是群，如$\langle \boldsymbol{P},\cdot\rangle$是可消半群，但不是群。对于有限半群，却有

定理 9 有限可消半群是群。

证明： 设 $G=\{a_1,a_2,\cdots,a_n\}$，任取 $a_k,a_h\in G$，集合 $\bar{G}=\{a_ka_1,a_ka_2,\cdots,a_ka_n\}$ 中任意两个元素都不相同。这是因为，如果有两个相同，如 $a_ka_i=a_ka_j$，则由消去律，推得 $a_i=a_j$。所以 $|\bar{G}|=n=|G|$。

另一方面，显然 $\bar{G}\subseteq G$。所以 $\bar{G}=G$。$\bar{G}$ 中必有一个是 a_h，即 a_k 是 a_h 的左因子。同样可知 a_k 是 a_h 的右因子。

这样，G 中任意两个元素都互相整除。由定理 3，G 是群。

证毕

五、元素的阶

设 a 是群 G 的一个元素．序列

$$a, a^2, a^3, \cdots \tag{8}$$

中第一个等于单位元 e 的元素(如果存在)设为 a^m，则称 a 为 m 阶元素。如果序列(8)中没有一个等于 e，那末 a 称为无限阶元素。

显然 e 的阶数是 1，它是唯一的 1 阶元。任意有限阶元素的阶数都是正整数。

在群 $\langle \mathbf{Z}, +\rangle$ 中，除单位元 0 外，都是无限阶元素。群 $\langle \mathbf{Q}^*, \cdot\rangle$ 中，除单位元 1 是 1 阶元和 -1 是 2 阶元外，其他元素 a 的任意正整数方幂都不等于 1，所以是无限阶的。

$U_4=\{1,-1,i,-i\}$ 组成的乘群中，1 的阶为 1，-1 的阶为 2，i 的阶为 4，$-i$ 的阶也为 4。

在§3·1例 4 的群中，a 是 1 阶元(单位元)；$b\neq a$，$b^2=a$，所以 b 是 2 阶元；同样可以知道，元素 c 和 d 都是 2 阶元。

阶是分析群中元素的工具。群里每个元素都有自己的阶(包括无限阶)，元素在群中的地位，以及元素之间的关系，可以在元素的阶上有所反映。例如，显然阶不大于 2 的元素与其逆元相同；任意元素与其逆元同阶。此外，有

定理 10 群的元素 a，如果满足 $a^m=e$，则其阶是 m 的因子。

证明：设 a 的阶为 n，如果 $n\nmid m$，则有 $m=kn+r, 0<r<n$，那末 $a^m=a^{kn}\cdot a^r=(a^n)^k\cdot a^r=e^k\cdot a^r=a^r$，即 $a^r=e$，与 a 的阶为 n 矛盾。

证毕

有限群的元素显然是有限阶的，但所有元素阶有限的群，却不一定是有限群。如设 U 是 $\mathbf{C}$ 中所有各次单位根组

成的集合，显然U是无限集，且关于乘法作成群，但其每个元素都是有限阶的。事实上，设$\varepsilon\in U$，不妨假定ε是n次单位根，那末ε在U中的阶不大于n。

习 题 3·2

1．设a是群中的无限阶元素，求证：当$m\neq n$时，$a^m\neq a^n$。

2．设群G的阶为偶数，求证：G中一定有二阶元，且二阶元的个数是奇数。

3．设群G中元素的阶不超过2，求证：G是可换群。

4．求证：群中幂等元(见复习题二第11题)只有单位元。

5．求证：群G是可换群当且仅当对于任何元素a，b，有$(ab)^2=a^2b^2$。

*6．求证：群中ab的阶等于ba的阶。

7．求证：群中阶数>2的元素个数若有限，必为偶数。

8．在群$\left\langle\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\},\cdot\right\rangle$中，每个元素的阶数=？。

9．设群G与$\bar{G}$同态，$a\in G$的阶为n，$\bar{a}$为a的同态象，求证：$\bar{a}$的阶$\leqslant n$。

10．求证：在可换群中ab的阶$\leqslant a$的阶·b的阶。

*11．在任意群中，求证：abc, bca, cab同阶。

*12．假如在半群A中存在元素d，它整除A的所有元

素，同时又可被所有元素整除，求证A是群。

13．求证：可换群是唯一分解半群。

14．求证：偶数阶群中含有$a\neq e$，$a^2=e$。

15．设p为素数．在可换群中，若a，b的阶都是p的方幂，求证ab的阶也是p的方幂。

§3·3　子　　群

为了剖析群的结构，必须研究群的子集．本节和下一节讨论群的两种类型的子集：子群和陪集。

一、子群

定义1　群$\langle G,\cdot\rangle$中，如果非空子集H关于群G的乘法也构成群，则$\langle H,\cdot\rangle$称为$\langle G,\cdot\rangle$的子群。

子群自然是子半群，即关于乘法封闭，但仅有这一点是不够的，如群$\langle \mathbf{Z},+\rangle$中，$\langle \mathbf{P},+\rangle$显然是子半群，但不是子群．那末，群的怎样的子集才是子群呢？

定理1　设H是群$\langle G,\cdot\rangle$的非空子集，则$\langle H,\cdot\rangle$为子群的充要条件是：

（1）如果a，$b\in H$，则$ab\in H$；

（2）$\langle G,\cdot\rangle$的单位元$e\in H$；

（3）如果$a\in H$，则$a^{-1}\in H$。

证明：必要性．

设$\langle H,\cdot\rangle$是子群，条件1显然成立．$\langle H,\cdot\rangle$的单位元设为e'，则$(e')^2=e'$．两端同乘e'在$\langle G,\cdot\rangle$中的逆元，得$(e')^2e'^{-1}=e'e'^{-1}$．即$e'=e\in H$．任取$a\in H$，$\langle H,\cdot\rangle$是群，

故存在 $a' \in H$，使 $a'a = aa' = e$，于是 a' 也是 a 在$\langle G,\cdot\rangle$中的逆元。逆元是唯一的，所以 $a' = a^{-1}$，即 $a^{-1}\in H$。

充分性。

由条件 1，$\langle H,\cdot\rangle$是群胚，结合律自然成立。又因条件 2、3，$\langle H,\cdot\rangle$是群，即$\langle G,\cdot\rangle$的子群。

证毕

任何群都有子群，例如这个群本身及单位元构成的单元素群都是子群，称为平凡子群，其他子群称为真子群。

如$\langle \mathbf{Z},+\rangle$是$\langle \mathbf{Q},+\rangle$的真子群，而后者又是$\langle \mathbf{R},+\rangle$的真子群。$\langle\{1,-1\},\cdot\rangle$ 是 $\langle U_4,\cdot\rangle$ 的真子群，$\langle U_4,\cdot\rangle$ 又是 $\langle U_8,\cdot\rangle$ 的真子群（见§3·1 例 3），这里 $U_4=\{1,-1,i,-i\}$，$U_8=\left\{1,\frac{1+i}{\sqrt{2}},i,\frac{-1+i}{\sqrt{2}},-1,\frac{-1-i}{\sqrt{2}},-i,\frac{1-i}{\sqrt{2}}\right\}$。

注意：群的子集有时虽作成群也不一定是子群，必须两者的代数运算一致才行。如 $\langle \mathbf{Q}^+,\cdot\rangle$ 是群，但不是$\langle \mathbf{Q},+\rangle$的子群，因为代数运算不同。

定理 1 还可再简化，即

定理 2 如果 H 是群$\langle G,\cdot\rangle$的非空子集，则 $\langle H,\cdot\rangle$是子群的充要条件是：

若 a，$b\in H$，则 $ab^{-1}\in H$。[注]

证明：假设$\langle H,\cdot\rangle$是子群，由定理 1，如果 $b\in H$，则 $b^{-1}\in H$，再设 $a\in H$，则 $ab^{-1}\in H$。

反之，在 H 中任取 a，由 $a\in H$，$a\in H$，得 $e=aa^{-1}\in H$，

注 可以理解为关于除法封闭。

而由 $e\in H$，$a\in H$，故 $a^{-1}=ea^{-1}\in H$. 这样，定理 1 的条件 2、3 都已适合.任取 $b\in H$,因而 $b^{-1}\in H$. 由 $a\in H, b^{-1}\in H$，又得 $ab=a(b^{-1})^{-1}\in H$. 根据定理 1，$\langle H,\cdot\rangle$是子群.

证毕

注意：对于加群，定理 2 的条件化为，

若 a，$b\in H$，则 $a-b\in H$.

定理 3 设 H_1 和 H_2 是群 G 的子群，则 $H_1\cap H_2$ 也是子群.

证明：$e\in H_1$，$e\in H_2$，故 $e\in H_1\cap H_2\neq\phi$. 现设 $a,b\in H_1\cap H_2$，自然 $a,b\in H_1$，由定理 2，$ab^{-1}\in H_1$. 同理 $ab^{-1}\in H_2$. 即 $ab^{-1}\in H_1\cap H_2$. 再据定理 2，$H_1\cap H_2$ 是群 G 的子群.

证毕

同样可以证明

定理 4 设 H_λ, $\lambda\in\Lambda$ 都是群 G 的子群，则 $\bigcap\limits_{\lambda\in\Lambda}H_\lambda$ 也是 G 的子群。

刚才说过，群的子半群不一定是子群，但对于有限群，却有

定理 5 有限群的子半群是子群.

证明：设 G 是有限群，H 是其子半群,因而是有限半群. 群 G 中消去律成立，所以 H 中消去律也成立. 由 §3·2 定理 9，H 作成群，即 G 的子群.

例 1 求证：集合 $H=\{(1,\ b)\mid b\in \mathbf{R}\}$ 构成 §3·1 例 5 中群$\langle \mathbf{R}^*\times\mathbf{R},\cdot\rangle$的子群.

证明：H 关于乘法封闭. 事实上，显然

$$(1,b_1)\cdot(1,b_2)=(1,b_1+b_2)\in H;$$

单位元$(1,0)\in H$；

$(1,b)$的逆元$(1,-b)\in H$。

由定理1，$\langle H,\cdot\rangle$是子群。

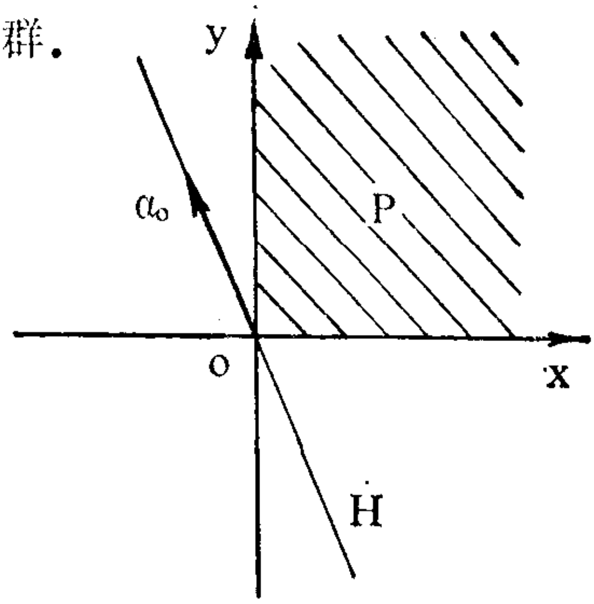


图3—2

例2 平面向量集合$\boldsymbol{R}_2$按向量加法作成群。设$\alpha_0\in\boldsymbol{R}_2$，$\alpha_0\neq 0$。求证：

(1) $H=\{\lambda\alpha_0\mid\lambda\in\boldsymbol{R}\}$作成子群；

(2) $P=\{(a,b)\mid a\geqslant 0,b\geqslant 0\}$不作成子群。(如图3—2)

证明：$\alpha_0\in H$，故$H\neq\phi$。任取α，$\beta\in H$，设$\alpha=\lambda\alpha_0$，$\beta=\mu\alpha_0$，则$\alpha-\beta=\lambda\alpha_0-\mu\alpha_0=(\lambda-\mu)\alpha_0\in H$。所以$\langle H,+\rangle$是$\langle\boldsymbol{R}_2,+\rangle$的子群。而$(1,1)\in P$，但其负元$(-1,-1)\notin P$，故$P$不是子群。

二、正规化子

一个群里与某一个固定元素a可换的元素（即适合$ax=xa$的元素x）总是有的，如单位元和a的方幂$a^n(n\in\boldsymbol{Z})$都是这样的元素。

定义2 群G中与$a\in G$可换的元素组成的集合记为$N(a)$，称为a的正规化子。

任意群的所有元素都与单位元e可换，所以$N(e)$等于整个群。对于可换群，显然任意元素的正规化子与群本身相

等。

定理 6 群中任意元素的正规化子是子群。

证明：$N(a)\neq\phi$，因为 $e\in N(a)$。如果 $x,y\in N(a)$，则

$$(xy)a=x(ya)=x(ay)=(xa)y=(ax)y=a(xy),$$

即 $xy\in N(a)$。如果 $x\in N(a)$，则 $xa=ax$，两端左、右各乘 x^{-1}，得 $x^{-1}xax^{-1}=x^{-1}axx^{-1}$，即 $ax^{-1}=x^{-1}a$，$x^{-1}\in N(a)$。由定理 1，$N(a)$是子群。

证毕

例 3 在 § 3·1 例 5 的群中，取 $a=(2,1)$，求 $N(a)$。

解：设$(x,y)\in N(a)$，则$(2,1)(x,y)=(x,y)(2,1)$。因而 $(2x,1\cdot x+y)=(x\cdot 2,y\cdot 2+1)$，$(2x,x+y)=(2x,2y+1)$，或 $x+y=2y+1$，$y=x-1$，即 $(x,y)=(x,x-1)$。

$$N(a)=\{(x,y)\mid x\in \boldsymbol{R}^*,\ y=x-1\}.$$

三、子群的乘积

定义 3 设K，H是群G的子集，集合

$$KH=\{kh\mid k\in K,\ h\in H\}$$

称为子集K与H的乘积。

定理 7 群的子集的乘法适合结合律：

$$(HK)L=H(KL). \qquad (1)$$

证明：左集的元素形如$(hk)l$，其中 $h\in H,K\in K,l\in L$。由于群元素乘法适合结合律，因而$(hk)l=h(kl)$也是(1)式右端集合的一个元素。同样可知右集的元素也是左集的元素。即(1)式成立。

证毕

两个子群的乘积不一定仍是子群。那末什么情况下两个

子群的乘积才是子群呢？

定理 8 假如K，H是群G的子群，则乘积KH是子群的充要条件是$KH=HK$。

证明：设KH是G的子群，任取$kh\in KH$，则$(kh)^{-1}\in KH$，因而有$k_1h_1\in KH$，使$(kh)^{-1}=k_1h_1$。

$$kh=(k_1h_1)^{-1}=h_1^{-1}k_1^{-1}\in HK,$$

即$KH\subseteq HK$，同样可证$KH\supseteq HK$，即$KH=HK$。

反之，假定$KH=HK$，任取$kh\in KH$，其逆元$h^{-1}k^{-1}\in HK=KH$，另外，单位元$e=ee\in KH$。下面证明KH关于乘法封闭。事实上，

$$\begin{aligned}(KH)(KH)&=(KH)(HK)=K(HH)K\\&\subseteq K(HK)=K(KH)=(KK)H\subseteq KH.\end{aligned}$$

因而KH是群G的子群.

（一个集合M关于乘法封闭，用集合乘积表示，即$MM\subseteq M$）

证毕

注意：$KH=HK$说明两个子群可换，并非指两子群中任意两个元素可换。也就是说，任取$k\in K$，$h\in H$，不一定有$kh=hk$，但一定存在$k_1\in K$，$h_1\in H$，使$kh=h_1k_1$。

对于可换群，任意两元素可换，因而任意两子群可换，所以可换群任意两子群的乘积还是子群。

在加群中，子集的乘积，应叫做子集的和，即$K+H=\{k+h|k\in K,h\in H\}$。

四、子群的生成系

设S是群G的非空子集，这时，一定存在包含S的子群，

例如G本身就是一个，包含S的所有子群的交(由定理4)也是G的子群．这个子群称为S生成的子群，记为$\langle S\rangle$．$\langle S\rangle$是包含S的最小子群．S称为子群$\langle S\rangle$的生成系．显然，当S本身就是子群时，$\langle S\rangle = S$．

S生成的子群$\langle S\rangle$中包含一些怎样的元素呢？

定理 9 设$S\subseteq G$，G是群，则$\langle S\rangle$由S的元素及其逆元素的任意有限乘积组成．

分析： 设$S=\{a, b, c, \cdots\}$．定理说$\langle S\rangle$将包括下形的一切元素：a，abc^{-1}，e，$b^{-3}ac^{-1}b^2$，$c^2b^{-1}c^2b^{-4}$，$\cdots$．

证明： 设$S=\{a, b, c, \cdots\}$．假定由a，b，c，$\cdots$，a^{-1}，b^{-1}，c^{-1}，$\cdots$中一切有限个元素的乘积形成的集合为P．

一方面，P关于G中乘法封闭，这是因为两个上述的积相乘，还是这样的乘积，且$S\subseteq P$．另外，P中任意元素的逆元显然也属于P．单位元$e=aa^{-1}\in P(a\in S)$．所以P是G的子群．

另外，任意包含S的子群显然也包含上述乘积，即包含P．

所以，$P=\langle S\rangle$．

证毕

例 4 $S=\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots\right\}$是$\langle \boldsymbol{R}, +\rangle$中子群$\langle \boldsymbol{Q}, +\rangle$的生成系．

分析：须证$\boldsymbol{Q}$的每个元素都可写成S中元素及其负元素的有限和．

证明：考虑任意有理数$\frac{n}{m}$．

如果 $n>0$，则

$$\frac{n}{m}=\overbrace{\frac{1}{m}+\cdots+\frac{1}{m}}^{n};$$

如果 $n<0$，则

$$\frac{n}{m}=\overbrace{\left(-\frac{1}{m}\right)+\cdots+\left(-\frac{1}{m}\right)}^{-n};$$

如果 $n=0$，则 $\frac{n}{m}=1+(-1)$。

所以，$\langle \boldsymbol{Q},+\rangle=\langle S\rangle$。

习 题 3·3

1．设 H 是群 G 的子群，K 是 H 的子群，求证：K 是 G 的子群，且 $KH=HK=H$。

2．设 S 是群 G 的子集，求证：与 S 中每个元素可换的元素作成 G 的子群。

3．如果 K，H 是群 G 的子群，$KH=HK$，求证：K 是 KH 的子群。

4．设 S 是群 G 的生成系，σ 是 G 到群 $\bar{G}$ 的满同态，求证：$\sigma[S]$ 是 $\bar{G}$ 的生成系。

5．在 $\langle \boldsymbol{C}^*,\cdot\rangle$ 中，求 $\langle i\rangle$，$\left\langle -\frac{1}{2}i\right\rangle$，$\langle 2,\ -5\rangle$，$\left\langle -\frac{1}{2}+\frac{\sqrt{3}}{2}i\right\rangle$。

6．求证：无限群有无限个子群。

7．求证：任意群可表为可换群的并集。

8. 求证：可换群中阶数不高于 2 的元素作成子群。

9. 求证：可换群中的有限阶元素构成一个子群。

10. 设 g 是群 G 的固定元素，H 是 G 的子群，求证：集合 $g^{-1}Hg=\{g^{-1}hg \mid h\in H\}$ 作成 G 的子群。

11. 在§3·1 例 5 的群中，求元素 (1，1) 的正规化子。

*12. 设 H_1，H_1'，H_2，H_2' 是 G 的子群，$H_1\subseteq H_1'$，$H_2\subseteq H_2'$，求证：$(H_1H_2)\cap H_1'\cap H_2'=(H_1\cap H_2')(H_1'\cap H_2)$。

13. 求证：群的有限子群胚是子群。

14. 设 H_1 和 H_2 是群 G 的子群。求证：$H_1\cup H_2$ 是子群的充要条件是 $H_1\subseteq H_2$ 或 $H_2\subseteq H_1$。

§3·4 陪　集

一、什么是陪集

在上节例 2 中，任取 $\beta\in \boldsymbol{R}_2$，则 $\beta+H$ 的元素是 β 与 H 中所有向量的和，即

$$\beta+H=\{\beta+\alpha \mid \alpha\in H\}.$$

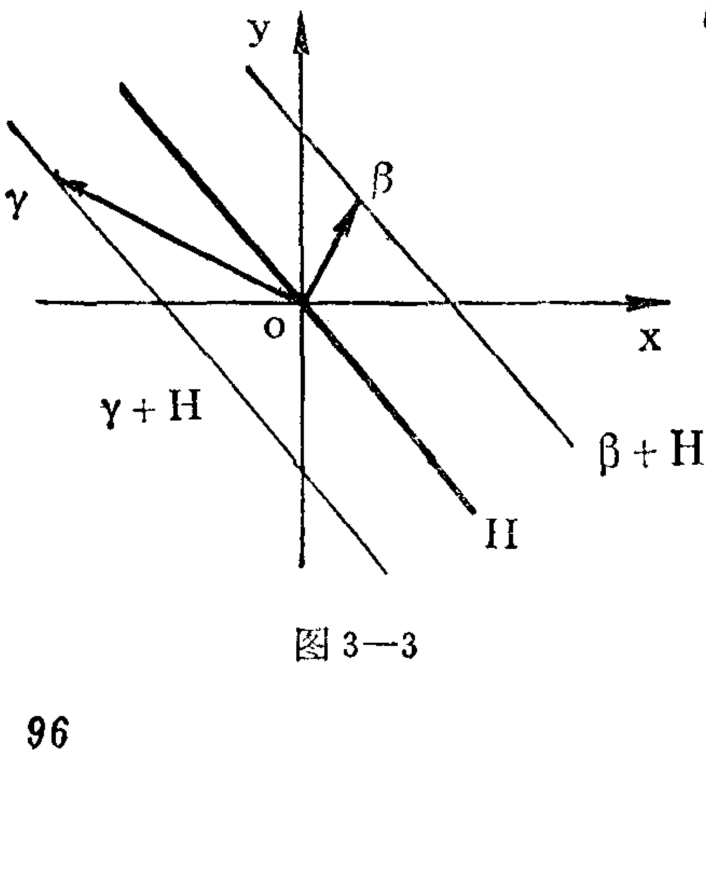


图 3—3

它代表平行 H 的一条直线。再任取 $\gamma\in \boldsymbol{R}_2$，则 $\gamma+H$ 也是一条平行直线。整个平面 $\boldsymbol{R}_2$，可以看作无穷多条平行直线的并集（如图 3—3）。这种思想可以推广到一般的群中。

定义 1 设 $\langle H,\cdot\rangle$

是群$\langle G,\cdot\rangle$的子群，$a\in G$，则集合乘积

$$aH=\{ah|h\in H\}$$

称为H在G中由a生成的左陪集。而集合乘积

$$Ha=\{ha|h\in H\}$$

称为H在G中由a生成的右陪集。如果左、右陪集相同：$aH=Ha$，则称为陪集。

例1 $\langle \mathbf{Z},+\rangle$是$\langle \mathbf{R},+\rangle$的子群，它在$\langle \mathbf{R},+\rangle$中由$a$生成的左陪集为

$a+\mathbf{Z}=\{\cdots,\ a-2,\ a-1,\ a,\ a+1,\ a+2,\ \cdots\}$，其元素之间相差一个整数(如图3—4)。

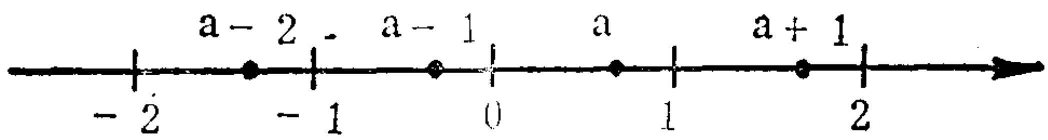


图3—4

这里由于运算可换，左陪集也是右陪集，即陪集。

下面的讨论针对左陪集，同样适用于右陪集。

二、左陪集的性质

群中的左陪集是一个子集，群中不同的元素可以属于同一个左陪集。

定理1 设H是群G的子群，a，$b\in G$，则a，b属于H的同一左陪集的充要条件是$a^{-1}b\in H$。

证明： 如果a，b属同一左陪集，则$aH=bH$，即任取$ah_1\in aH$，必有$bh_2\in bH$，使$bh_2=ah_1$。由此可得$a^{-1}b=h_1h_2^{-1}\in H$。

反之，如果$a^{-1}b=h_0\in H$，则$a=bh_0^{-1}$.任取$ah\in aH$，则

$ah=bh_0^{-1}h$。由于 $h_0^{-1}h\in H$，故 $ah\in bH$，$aH\subseteq bH$。同样可证 $bH\subseteq aH$。即 $aH=bH$，a 与 b 在一个左陪集中。

证毕

例 2 在§3·1的例4中，$\{a,b\}$ 作成 G 的子群，设它为 H。现在考查 H 在 G 中由4个元素生成的左陪集。

$$aH=\{a^2,ab\}=\{a,b\};$$
$$bH=\{ba,b^2\}=\{b,a\};$$
$$cH=\{ca,cb\}=\{c,d\};$$
$$dH=\{da,db\}=\{d,c\}.$$

因而 $aH=bH=H$，$cH=dH$ 是全部左陪集。a，b 在同一左陪集中，c，d 在同一左陪集中。我们看到，全体左陪集刚好是 G 的一种分类，这个事实对一般的群也是正确的。

定理 2 设 H 是群 G 的子群，则

(1) 对于任意的 $a\in G$，有左陪集包含 a；

(2) 两个左陪集要么相等，要么不相交。

证明： (1) 显然 $a\in aH$。

(2) 设 $aH\cap bH\neq\phi$，则有 h_1，$h_2\in H$，使 $ah_1=bh_2$，因而 $a=bh_2h_1^{-1}$。H 是子群，故有 $h_2h_1^{-1}\in H$，即 $a\in bH$。设 $a=bh_0$，那末任取 $ah\in aH$，则 $ah=bh_0h\in bH$。所以 $aH\subseteq bH$，同理可证 $bH\subseteq aH$，因而 $aH=bH$。

证毕

所以，群 G 的子群 H 的所有左陪集是 G 的一种分类。

在群的子群的左陪集之中，有且只有一个左陪集是子群，这就是单位元所在的左陪集。

作子群 H 到任一陪集 aH 的映射为：$\sigma(h)=ah$。显然 σ 是满射，又因群中有消去律，所以，如果 $h_1\neq h_2$，则 ah_1

$\neq ah_2$. σ 是一一映射，$H \sim aH$. 所以，群关于任一子群的所有左陪集彼此等势. 这是左陪集分类的特点.

例 3 在 6 次单位根乘群 $\langle U_6, \cdot \rangle$ 中，设 $H = \{\varepsilon_0, \varepsilon_3\}$，则 H 是子群. H 的左陪集共三个：

$$\varepsilon_0 H = \varepsilon_3 H = H = \{\varepsilon_0, \varepsilon_3\};$$

$$\varepsilon_1 H = \varepsilon_4 H = \{\varepsilon_1, \varepsilon_4\};$$

$$\varepsilon_2 H = \varepsilon_5 H = \{\varepsilon_2, \varepsilon_5\}.$$

每个左陪集含两个元素，$U_6 = \varepsilon_0 H \cup \varepsilon_1 H \cup \varepsilon_2 H$.

一般地，由定理 2，群都可以表成任一子群所有左陪集的并：

$$G = \bigcup_{a \in G} aH,$$

常称之为群关于一个子群的左陪集分解.

当 G 为有限群时，它关于子群 H 的左陪集分解为：

$$G = a_1 H \cup a_2 H \cup a_3 H \cup \cdots \cup a_k H.$$

这里 k 是不同左陪集的个数，称为 H 在 G 中的指数，记为 $(G:H)$.

当 $H = G$ 时，显然 $(G:G) = 1$；当 $H = \{e\}$ 时，$(G:\{e\}) = |G|$. 总之，子群越大，指数越小.

设 $|G| = n$，$|H| = m$，那末

$$|a_1 H| = |a_2 H| = \cdots |a_k H| = m.$$

$$n = |G| = m + m + \cdots + m = km.$$

由此得到著名的拉格朗日(Lagrange)[注]定理：

定理 3 有限群 G 的阶等于其子群 H 的阶与指数之积，

注 J. Lagrange(1736—1813)，法国数学家.

即 $|G| = |H| \cdot (G:H)$。

如例 3 中，$|G|=6$，$|H|=2$，H 的指数为 3（$6=2\cdot3$）。

三、拉格朗日定理的应用

从拉格朗日定理可知，有限群的子群阶总是群阶的因子。例如 4 阶群不会有 3 阶子群；而 5 阶群只有平凡子群，这因为 5 的正整数因子只有 5 和 1，子群的阶只能是 5 或 1，若是 5，即子群为群本身；若是 1，即子群为单位元群。

有限群中每个元素的阶与群阶有着简单的关系：

定理 4 有限群中元素的阶是群阶的因子。

证明：设 a 是有限群 G 的 m 阶元素，子集

$$H=\{a,\ a^2,\cdots,a^m=e\}$$

显然是 G 的子群。由定理 3，$|H|\,\big|\,|G|$，即 $m\,\big|\,|G|$。

证毕

如 $\langle U_6,\cdot\rangle$ 中，ε_0 是 1 阶元，ε_1，ε_5 是 6 阶元，ε_2，ε_4 是 3 阶元，ε_3 是 2 阶元，它们的阶都是 $|U_6|=6$ 的因子。

由定理 4 立即可知 n 阶群中每个元素的 n 次方幂都等于 e。

为了论述方便，本节讨论都是针对左陪集的，上面对左陪集的结果对右陪集也适合（只是定理 1 的条件应改为 $ba^{-1}\in H$），可请读者一一验证。

习 题 3·4

1. 设 H 是群 G 的子群，求证 a，b 属于同一右陪集的充要条件是 $ba^{-1}\in H$。

2. 本节定理 2 中将“左陪集”换为“右陪集”仍成立。

试证明之。

3．求证：可换群的任何子群的左、右陪集相等。

*4．设H是群G的子群，K是H的子群，求证：$(G:K)=(G:H)(H:K)$。

5．求证：一个子群的左陪集元素的逆元组成这个子群的一个右陪集。

6．设群G的阶为素数，求证：G没有真子群。

7．设H_1，H_2是群G的子群，求证：$H_1\cap H_2$的任意左陪集是H_1的一个左陪集与H_2的一个左陪集之交。

8．证明：p^n阶（p为素数）群中必有p阶元素。

9．在§3·1例5中，取$H=\{(x,0)|x\in \boldsymbol{R}^*\}$，求证：$H$是$\langle \boldsymbol{R}^*\times \boldsymbol{R},\cdot\rangle$的子群．求（1,1）的左陪集和右陪集。

10．找出克莱茵四元群B_4（§3·1例4）的所有真子群。

11．设H是群G的指数为2的子群，则H的左、右陪集相等。

§3·5　循　环　群

这一节，介绍一类最简单最基本的群，也是解决得最彻底的群，这就是循环群。

一、什么是循环群

设S是群G的子集，如果S生成的子群是G本身，即$\langle S\rangle=G$，则称S是群的生成系．当生成系只含一个元素时，称G为循环群．显然，循环群是可换群．设$G=\langle a\rangle$，则a称为G的生成元．这时，显然

$$G=\{\cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots\}.$$

如果 a 的不同方幂互不相同，则 G 是一个无限群，称为无限循环群。如果 G 中有两个方幂相同，如 $a^i=a^j(i>j)$，则 $a^{i-j}=e$，说明 a 是有限阶元素，其阶为 $i-j$ 的因子。这时 G 中仅有有限个不同的元素：$a, a^2, \cdots, a^n=e$，这里 n 是 a 的阶。a 的所有整数方幂不过是上面 n 个元素的周期循环而已。这时 G 称为有限循环群，精确地说，是 n 阶循环群。

例 1 $\langle \mathbf{Z}, +\rangle$ 是无限循环群，1 是生成元，$2=1+1$ 是 1 的 2 次方幂注，$3=1+1+1$ 是 1 的 3 次方幂，…，0 是 1 的零次方幂，-1 是 1 的 -1 次方幂，$-2=(-1)+(-1)$ 是 1 的 -2 次方幂，…。即 $\langle \mathbf{Z}, +\rangle=\langle 1\rangle$。

例 2 $\langle U_n, \cdot\rangle$ 是 n 阶循环群，ε_1 是生成元。事实上，

$$\varepsilon_1^k=\left(\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}\right)^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}=\varepsilon_k,\ k=0,$$

$\pm 1, \pm 2, \cdots$。$\varepsilon_1, \varepsilon_1^2, \cdots, \varepsilon_1^n$ 刚好是组成 U_n 的全部元素。如果 k 再由 n 继续增大，或从 1 减小，则 ε_1^k 又周而复始地循环起来。

例 1 和例 2 实际上概括了所有的循环群。

定理 1 无限循环群都同构于 $\langle \mathbf{Z}, +\rangle$。

证明： 设 $\langle a\rangle$ 是无限循环群，作 $\langle a\rangle$ 到 $\mathbf{Z}$ 的对应法则 σ 如下：$\sigma(a^k)=k, k\in\mathbf{Z}$。

由于 a 的不同方幂互不相同，所以 σ 是映射，且显然是满射。又如果 $a^k\neq a^h$，则显然 $k\neq h$，故 σ 是单射。总之，σ 是一一映射。

注 这里的“方幂”即倍数，凡加群的方幂 a^n 以后记为 na。

又因

$$\sigma(a^k \cdot a^h) = \sigma(a^{k+h}) = k+h$$
$$= \sigma(a^k) + \sigma(a^h),$$

所以 σ 是同态．因而 σ 是同构，即 $\langle a\rangle \cong \langle \mathbf{Z}, +\rangle$.

证毕

定理 2 n 阶循环群同构于 $\langle U_n, \cdot\rangle$.

证明： 设 $\langle a\rangle$ 是 n 阶循环群：

$$\langle a\rangle = \{a, a^2, \cdots, a^{n-1}, a^n = e\}.$$

作 $\langle a\rangle$ 到 U_n 的对应法则 σ 如下：$\sigma(a^k) = \varepsilon_k$, $k = 1, 2, \cdots, n-1, n$.

σ 是映射．事实上，如果 $a^k = a^h$，则 $a^{k-h} = e$，即 $n | k-h$，因而 $\varepsilon_1^{k-h} = 1$，这时

$$\varepsilon_k = \varepsilon_1^k = \varepsilon_1^{h+(k-h)} = \varepsilon_1^h \cdot \varepsilon_1^{k-h} = \varepsilon_1^h = \varepsilon_h,$$

即 $\sigma(a^k) = \sigma(a^h)$.

σ 是满射．事实上，任取 $\varepsilon_k \in U_n$，则 $\sigma(a^k) = \varepsilon_k$, $a^k \in \langle a\rangle$.

σ 是单射．事实上，如果 $a^k \neq a^h$，则 $n \nmid k-h$，因而 $\varepsilon_1^k \neq \varepsilon_1^h$, $\varepsilon_k \neq \varepsilon_h$, $\sigma(a^k) \neq \sigma(a^h)$.

σ 是同态．事实上，任取 $a^k, a^h \in \langle a\rangle$,

$$\sigma(a^k \cdot a^h) = \sigma(a^{k+h}) = \varepsilon_{k+h} = \varepsilon_1^{k+h}$$
$$= \varepsilon_1^k \cdot \varepsilon_1^h = \varepsilon_k \cdot \varepsilon_h = \sigma(a_k) \cdot \sigma(a_h).$$

因而 σ 是同构映射，即 $\langle a\rangle \cong \langle U_n, \cdot\rangle$.

证毕

无限循环群常记为 C_∞，n 阶循环群常记为 C_n．从同构的观点看，循环群只不过两种，一种是整数群 $\langle \mathbf{Z}, +\rangle$，另一种是 n 次单位根乘群 $\langle U_n, \cdot\rangle$．任意循环群都同构于它们．所

以，可以说，只要掌握了这两种群，就等于掌握了所有循环群。

在无限循环群$\langle a\rangle$中，当$k\neq h$时，$a^k\neq a^h$，所以它的每个元素对应唯一的形式a^k。

在n阶循环群中就不同了，这时，$\langle a\rangle=\{a, a^2, \cdots, a^n=e\}$。而

$$a^{n+1}=a^n\cdot a=a,\quad a^{n+2}=a^2,\ \cdots$$

$$a^{-1}=a^{n-1},\quad a^{-2}=a^{n-2},\ \cdots$$

因而$\langle a\rangle$中每个元素表为a的方幂时，有无穷多种形式。如3阶循环群中：

$$\cdots=a^{-5}=a^{-2}=a=a^4=a^7=\cdots,$$

$$\cdots=a^{-4}=a^{-1}=a^2=a^5=a^8=\cdots,$$

$$\cdots=a^{-6}=a^{-3}=a^0=a^3=a^6=\cdots.$$

一般地，n阶循环群$\langle a\rangle$中元素a^k可表为

$$\cdots=a^{-2n+k}=a^{-n+k}=a^k=a^{n+k}=a^{2n+k}=\cdots.$$

同一元素表为a的方幂时，有且仅有一个方幂的指数是不大于n的正整数。下面约定，n阶循环群$\langle a\rangle$中，每个元素都用这种指数的方幂表示，于是就使元素有了唯一确定的形式。

二、循环群的子群

群论中一个重要而又困难的问题是找出已知群的所有子群。对循环群来说，这个问题是十分简单的。为了解决这一问题，首先证明

引理1 设a是群G的元素，且H是包含a的子群，则a生成的循环群是H的子群，即$\langle a\rangle\subseteq H$。

证明： 由于$a\in H$，则$a^n=a\cdot a\cdots a\in H$，$e=a^0\in H$，

$a^{-1}\in H$，$a^{-n}=(a^{-1})(a^{-1})\cdots(a^{-1})\in H$，其中 n 为正整数．因而，$\langle a\rangle\subseteq H$。

证毕

定理 3 设$\langle a\rangle$为无限循环群，则其任意子群是且仅是形如$\langle a^k\rangle$的循环群，其中 k 是任意整数．除单位元群$\langle a^0\rangle$外，其他子群都是无限循环群．

分析：证明分两方面．第一，证明G的每个子群形如$\langle a^k\rangle$；第二，证明$\langle a^k\rangle$是G的子群．这里 k 是任意整数．

证明：(1) 设H是$\langle a\rangle$的任一子群．如果 $H=\{e\}$，则 $H=\langle a^0\rangle$．否则，H 中 a 的正整数方幂中必有最小指数，设为 k．下面证明$\langle a^k\rangle=H$．

$a^k\in H$，由引理 1，$\langle a^k\rangle\subseteq H$．反之，任取 $a^s\in H$，如果 $k\nmid s$，则可表 $s=qk+r$，其中 $0<r<k$．因而

$$a^r=a^{s-qk}=a^s\cdot(a^k)^{-q}\in H.$$

$0<r<k$，与 k 的取法矛盾，所以 $k|s$，$a^s\in\langle a^k\rangle$，$H\subseteq\langle a^k\rangle$．

总之，$H=\langle a^k\rangle=\{\cdots,\ a^{-2k},\ a^{-k},\ a^0,\ a^k,\ a^{2k},\ \cdots\}$．此外，显然 $H=\langle a^{-k}\rangle$．同一个子群有且仅有两个表示方法：$H=\langle a^k\rangle=\langle a^{-k}\rangle$．除$\langle a^0\rangle$外，$\langle a^k\rangle$显然是无限循环群．

(2) 任取整数 k，则 $a^k\in\langle a\rangle$，由引理 1，$\langle a^k\rangle$是$\langle a\rangle$的子群．

证毕

定理 4 设 $\langle a\rangle=\{a,\ a^2,\ \cdots,\ a^n=e\}$ 为 n 阶循环群，则其任意子群是且仅是形如$\langle a^k\rangle$的循环群，其中 k 是 n 的正因子．$\langle a^k\rangle$的阶等于$\frac{n}{k}$．

证明：(1) 设 $H=\{a^{k_1},\ a^{k_2},\cdots,a^{k_m}\}$ 是任一子群，其中 k_1，k_2，…，k_m 是不大于 n 的正整数．取 $k=\min\{k_1,k_2,$

$\cdots, k_m\}$. 下面证明 $H=\langle a^k\rangle$. 首先，因为 $a^k\in H$，故 $\langle a^k\rangle\subseteq H$. 其次，任取 $a^s\in H$，则可表 $s=qk+r$，其中 $0\leqslant r<k$. 因而 $a^r=a^{s-qk}=a^s\cdot(a^k)^{-q}\in H$. 如果 $r\neq 0$，则与 k 的最小性矛盾. 因而 $k|s$. 即 $a^s\in\langle a^k\rangle$，$H\subseteq\langle a^k\rangle$. 所以 $H=\langle a^k\rangle$ 是 $\langle a\rangle$ 中的循环子群.

(2) 任取 n 的正因子 k，显然 $\langle a^k\rangle$ 是 $\langle a\rangle$ 的子群.

(3) $\langle a\rangle$ 的任一子群 $\langle a^k\rangle=\{a^k, a^{2k}, \cdots, a^n\}$ 的阶等于 $\frac{n}{k}$.

证毕

以上两个定理揭示了循环群子群的形式. 因而，无限循环群 $\langle a\rangle$ 的子群有无限多个：

$$\{e\},\ \langle a\rangle,\ \langle a^2\rangle,\ \langle a^3\rangle,\ \cdots$$

n 阶循环群 $\langle a\rangle$ 的子群与 n 的正因子的个数一样多. 如 $|\langle a\rangle|=12$，则因 12 有 6 个正因子：1，2，3，4，6，12，因而 $\langle a\rangle$ 的子群有 6 个，即：

$\langle a\rangle=\{a,\ a^2,\ \cdots,\ a^{12}\}$，阶为 12；

$\langle a^2\rangle=\{a^2,\ a^4,\ \cdots,\ a^{12}\}$，阶为 6；

$\langle a^3\rangle=\{a^3,\ a^6,\ \cdots,\ a^{12}\}$，阶为 4；

$\langle a^4\rangle=\{a^4,\ a^8,\ a^{12}\}$，阶为 3；

$\langle a^6\rangle=\{a^6,\ a^{12}\}$，阶为 2；

$\langle a^{12}\rangle=\{a^{12}\}$，阶为 1.

这些子群的单位元是 $a^{12}=a^0=e$.

习 题 3·5

1. 设 $d|n$，求证：C_n 有 d 阶子群.

2. 求证：循环群的同态象也是循环群.

3. 设$m|n$，求证：C_n中方程$x^m=e$在G中有m个解.

4. 怎样的群只有一个子群？怎样的群只有两个子群？

5. 求证：n阶群是循环群当且仅当它有n阶元. 由此证明素数阶群是循环群.

6. 设G是可换群，H和K是有限循环子群，$|H|=r$，$|K|=s$，求证：如果r与s互素，则G包含rs阶循环子群。

7. 设$\langle a\rangle$为n阶循环群，求证：$\langle a^m\rangle=\langle a\rangle\Longleftrightarrow(m, n)=1$.

*8. 求证：$\mathbf{Z}[i]=\{a+bi|a, b\in\mathbf{Z}\}$关于加法作成的群不是循环群.

§3·6 变 换 群

一、从变换半群到变换群

设A是一个非空集合. 现在把A的每个变换当成一个元素，A中的全体变换组成一个集合，记为$\mathbf{S}(A)$. 两个变换σ和τ按照变换的乘法，又可得到A中的变换$\sigma\tau$. 变换的乘法适合结合律，所以$\langle\mathbf{S}(A),\cdot\rangle$是半群，称为集合$A$的变换半群，其单位元是恒等变换$\varepsilon_A$.

例1 设$A=\{1,2\}$，则$\mathbf{S}(A)$包含四个变换：

$$\sigma_1:\ 1\to1,\ 2\to1;$$
$$\sigma_2:\ 1\to1,\ 2\to2;$$
$$\sigma_3:\ 1\to2,\ 2\to1;$$
$$\sigma_4:\ 1\to2,\ 2\to2.$$

其中σ_2是恒等变换. $\mathbf{S}(A)$的乘法表如下：

·	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_1	σ_1	σ_1
σ_2	σ_1	σ_2	σ_3	σ_4
σ_3	σ_4	σ_3	σ_2	σ_1
σ_4	σ_4	σ_4	σ_4	σ_4

一般说来，给出一个集合A，就决定了一个有单位元的半群$S(A)$，这样的半群总有可逆元。那末哪些变换是这个半群的可逆元呢？我们知道，所谓σ是可逆元是指存在$\tau\in S(A)$，使$\sigma\tau=\tau\sigma=\varepsilon_A$（单位元），由§1·2推论1，这等价于说$\sigma$为一一变换。就是说，$S(A)$的可逆元群由所有一一变换组成，这个群显然由集合$A$所唯一确定，记为$G(A)$。$G(A)$是$S(A)$的子群，其单位元即$S(A)$的单位元——恒等变换$\varepsilon_A$。$\sigma\in G(A)$的逆元是$\sigma$的逆变换$\sigma^{-1}$，它也是一个一一变换（见§1·2六），因而在$G(A)$中，作为群中的逆元与作为变换的逆变换刚好是一致的。$\langle G(A),\cdot\rangle$的任意子群，叫做集合$A$的变换群。显然$G(A)$以及$\{\varepsilon_A\}$都是变换群。

上例中，σ_1和σ_4不是一一变换，而σ_2和σ_3都是一一变换，因而$G(A)=\{\sigma_2,\sigma_3\}$。

由子群的判别条件（§3·3定理2），得

定理1 集合A的某些一一变换组成的集合H作成变换群的充要条件是：

如果σ，$\tau\in H$，则$\sigma\tau^{-1}\in H$。

例2：平面R_2上的所有平移变换都可表为：$\sigma_{(a,b)}(x,y)=(x+a,y+b)$，这里$(a,b)$代表每个点$(x,y)$的平移大小。取不同的$(a,b)$，形成不同的平移变换。平移变换，显然是$R_2$的一一变换。记平移变换集为$T$，下面证明$T$作成$R_2$的变换群。

事实上，任取$\sigma_{(a,b)}$，$\sigma_{(c,d)}\in T$，则$\sigma_{(c,d)}$的逆元为

$\sigma_{(-c,-d)}$, $\sigma_{(a,b)}\cdot\sigma_{(c,d)}^{-1}=\sigma_{(a,b)}\cdot\sigma_{(-c,-d)}=\sigma_{(a-c,b-d)}\in\boldsymbol{T}$. 由定理1知，$\boldsymbol{T}$ 作成 $\boldsymbol{R}_2$ 的变换群.

例 3　平面 $\boldsymbol{R}_2$ 上的所有绕 O 点的旋转变换，都可表为：$\tau_\theta(x,y)=(x\cos\theta+y\sin\theta,-x\sin\theta+y\cos\theta)$，这里 θ 代表旋转的角度。不管 θ 等于多少，τ_θ 都是 $\boldsymbol{R}_2$ 的一一变换. 记旋转变换集为 $\boldsymbol{B}$，下面证明 $\boldsymbol{B}$ 作成 $\boldsymbol{R}_2$ 的变换群.

事实上，任取 τ_{θ_1}，$\tau_{\theta_2}\in\boldsymbol{B}$，则 τ_{θ_2} 的逆元为 $\tau_{-\theta_2}$，$\tau_{\theta_1}\cdot\tau_{\theta_2}^{-1}=\tau_{\theta_1}\cdot\tau_{-\theta_2}=\tau_{\theta_1-\theta_2}\in\boldsymbol{B}$. 由定理1知，$\boldsymbol{B}$ 作成 $\boldsymbol{R}_2$ 的变换群.

例 4　设想一个正方形纸板(如图 3—5)，考虑保持其外形不变的所有变换. 用 $R_{\frac{\pi}{2}}$，R_π，$R_{\frac{3}{2}\pi}$，$R_{2\pi}$ 表示正方形绕中心按顺时针方向分别转 $\frac{\pi}{2}$，π，$\frac{3}{2}\pi$，2π 的旋转；用 D_1，D_2 分别表示绕两条对角线的翻转，用 H，V 分别表示绕中心水平线和中心竖直线的翻转.

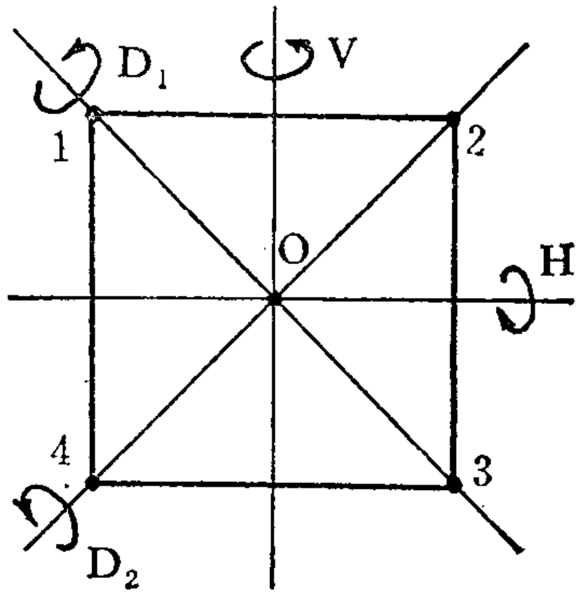


图 3—5

$R_{2\pi}$ 是恒等变换. 显然，$R_\pi=R_{\frac{\pi}{2}}^2$，$R_{\frac{3}{2}\pi}=R_{\frac{\pi}{2}}^3$，$R_{2\pi}=R_{\frac{\pi}{2}}^4$. 乘积 $R_{\frac{\pi}{2}}\cdot H$ 表示先绕水平线翻转，再旋转$\frac{\pi}{2}$，显然正与 D_1 相同，于是得到 $R_{\frac{\pi}{2}}\cdot H=D_1$.

同样可以分别作出它们两两乘积，得到下表：

$\cdot$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	H	V	D_1	D_2
$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	$R_{\frac{\pi}{2}}$	D_1	D_2	V	H
R_{π}	$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	$R_{\frac{\pi}{2}}$	R_{π}	V	H	D_2	D_1
$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3}{2}\pi}$	D_2	D_1	H	V
$R_{2\pi}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	H	V	D_1	D_2
H	D_2	V	D_1	H	$R_{2\pi}$	R_{π}	$R_{\frac{3}{2}\pi}$	$R_{\frac{\pi}{2}}$
V	D_1	H	D_2	V	R_{π}	$R_{2\pi}$	$R_{\frac{\pi}{2}}$	$R_{\frac{3}{2}\pi}$
D_1	H	D_2	V	D_1	$R_{\frac{\pi}{2}}$	$R_{\frac{3}{2}\pi}$	$R_{2\pi}$	R_{π}
D_2	V	D_1	H	D_2	$R_{\frac{3}{2}\pi}$	$R_{\frac{\pi}{2}}$	R_{π}	$R_{2\pi}$

这8个变换关于乘法封闭。R_{π}，$R_{2\pi}$，H，V，D_1，D_2 均为自身的逆元，而 $R_{\frac{\pi}{2}}^{-1}=R_{\frac{3}{2}\pi}$。因此它们作成变换群，称为正方形对称群，记为 D_4。D_4 不是可换群，如

$$R_{\frac{\pi}{2}}\cdot H\neq H\cdot R_{\frac{\pi}{2}}.$$

D_4 也不是循环群，但 D_4 的许多子群是循环群，如 $\{R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3}{2}\pi}, R_{2\pi}\}$，$\{R_{\pi}, R_{2\pi}\}$，$\{H, R_{2\pi}\}$，$\{V, R_{2\pi}\}$，$\{D_1, R_{2\pi}\}$，$\{D_2, R_{2\pi}\}$ 都是循环群。

二、群的正则实现

从历史上看，变换群的出现先于抽象群。变换群一方面是群的特例，另一方面，实际上也囊括了所有的群。下面的

凯莱(Cayley) 定理说明了这一点.

定理 2 每个群同构于一个变换群.

分析：让 $g\in G$ 对应 G 的左乘变换 π_g，π_g 是一一变换，$g\to\pi_g$ 是 G 到 $\mathbf{G}(G)$ 的单同态，全体 π_g 作成 $\mathbf{G}(G)$ 的子群胚，因而是与 G 同构的变换群.

证明：设 g 是群 G 的任一元素，定义 G 的左乘变换 $\pi_g:\pi_g(x)=gx$，$(x\in G)$. π_g 是满射，事实上，对于 $y\in G$，$g^{-1}y\in G$，而

$$\pi_g(g^{-1}y)=g(g^{-1}y)=y.$$

π_g 是单射. 事实上，如果 $x_1\neq x_2$，则 $gx_1\neq gx_2$，因而 $\pi_g(x)\neq\pi_g(x_2)$. 所以 π_g 是一一变换，$\pi_g\in\mathbf{G}(G)$.

作 G 到 $\mathbf{G}(G)$ 的映射 $\varphi:\varphi(g)=\pi_g$，$(g\in G)$. $\varphi[G]=\{\pi_g\mid g\in G\}$. 当 $g_1\neq g_2$，$g_1x\neq g_2x$，即

$$\varphi(g_1)=\pi_{g_1}\neq\pi_{g_2}=\varphi(g_2),$$

φ 为单射.

$$(\pi_g\pi_h)(x)=\pi_g(\pi_h(x))=\pi_g(hx)=ghx=\pi_{gh}(x),$$

故 $\varphi(gh)=\pi_{gh}=\pi_g\pi_h=\varphi(g)\varphi(h)$. 因而 φ 是 G 到 $\mathbf{G}(G)$ 的单同态. 显然 $\varphi[G]$ 是关于变换的乘法封闭，即作成子群胚，G 与 $\varphi[G]$ 同态，由§ 2·4 定理 1 不难看出，$\varphi[G]$ 作成子群，即为 G 的变换群，且与 G 同构.

证毕

任何一个群与其左乘变换群的同构映射 φ，称为群的正则实现.

例 5 写出群 $\langle\mathbf{R}_2,+\rangle$ 的正则实现.

解：每个 $\mathbf{R}_2$ 中的元素，对应 $\mathbf{R}_2$ 的一个左乘变换，这里的“左乘”应换为“左加”.

任取$(a,b)\in \boldsymbol{R}_2$，作左加变换$\sigma_{(a,b)}$如下：

$$\sigma_{(a,b)}(x,y)=(a,b)+(x,y)=(a+x,b+y).$$

相当于将任意点(x,y)平移(a,b)。因而，$\langle \boldsymbol{R}_2,+\rangle$的左加变换群就是平移变换群$\boldsymbol{T}$。因此，$(a,b)\to\sigma_{(a,b)}$是$\langle \boldsymbol{R}_2,+\rangle$的正则实现，它是$\langle \boldsymbol{R}_2,+\rangle$到平移变换群的同构映射。

习　题　3·6

1．用凯莱定理证明阶数相同互不同构的有限群只有有限个。

2．写出D_4的所有子群.

3．写出D_4中R_π、D_1、H、V的正规化子。

4．求证：$\{R_{\frac{\pi}{2}},H\}$是D_4的生成系。

5．设$a\in A$，求证：A的所有使a不动的一一变换的集合是A的变换群。

6．写出C_n的正则实现．

7．写出$\langle \boldsymbol{Z},+\rangle$的正则实现．

8．平面上全体轴对称变换是否作成变换群？

9．找出例1的半群$S(A)$中的左零元.它有没有右零元？

10．$\boldsymbol{R}$中全体以下形式的变换

$$\tau_{(a,b)}(x)=ax+b(a\neq 0,\ a,b\in \boldsymbol{R})$$

作成$\boldsymbol{R}$的变换群，它与§3·1例5的群反向同构.试证明之。

§3·7　置　换　群

现在我们讨论一类特殊的变换群——置换群，它们是有限集上的变换群。

一、置换与置换群

设A是有限集，它的元素记成1，2，…，n．A的每个变换τ，可以用以下方式表示：

$$\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},\tag{1}$$

每个下面的元素是上面对应元素的象，即

$$\tau(1)=i_1,\ \tau(2)=i_2,\ \cdots,\ \tau(n)=i_n.$$

由于τ是一一变换，$\{i_1,\ i_2,\ \cdots,\ i_n\}=\{1,\ 2,\ \cdots,n\}$，所以$i_1i_2\cdots i_n$是1，2，…，$n$的一个排列．

如$\tau=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$表示$\tau(1)=3$，$\tau(2)=2$，$\tau(3)=1$．

这个变换也可以写成

$$\begin{pmatrix}1 & 3 & 2\\ 3 & 1 & 2\end{pmatrix},\ \begin{pmatrix}3 & 1 & 2\\ 1 & 3 & 2\end{pmatrix},\ \begin{pmatrix}2 & 1 & 3\\ 2 & 3 & 1\end{pmatrix}$$

等形式．只要象与原象的对应关系保持不变，就是同一个变换．

定义1　有限集的一一变换，称为置换．该有限集所含元素的个数，称为置换的次数．由某些n次置换组成的变换群，称为一个n次置换群．全体n次置换组成的置换群，称为n次对称群．n次对称群常记为S_n．

如

$$S_1=\left\{\begin{pmatrix}1\\ 1\end{pmatrix}\right\},$$

$$S_2=\left\{\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix},\ \begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\right\},$$

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\right.$$
$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$
$$\left.\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}.$$

n 个元素的全排列有 $n!$ 种，所以 S_n 共有 $n!$ 个元素。n 次置换群的阶永远不会超过 $n!$.

置换是变换，其乘法与一般的变换相同，但由于置换中元素的对应关系已直接写出，所以置换乘法的计算很方便。如

$$\pi=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix},\quad \sigma=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},$$

其积 $\pi\sigma$ 是连续实行 σ 和 π 两个置换的结果：

$$\begin{array}{c} \quad\sigma\quad\quad\pi \\ 1\longrightarrow4\longrightarrow4 \\ 2\longrightarrow3\longrightarrow2 \\ 3\longrightarrow2\longrightarrow1 \\ 4\longrightarrow1\longrightarrow3 \end{array}$$

即 $\pi\sigma=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$.

同样，可以算出 $\sigma\pi=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$.

由此也看出置换乘法是不可换的.

置换的逆变换，称为逆置换. n 次置换的逆置换，也是 n 次置换. 如上面 π 的逆置换是

$$\pi^{-1}=\begin{pmatrix}3&1&2&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}.$$

此外，n 次置换的任何整数方幂也都是 n 次置换．如

$$\pi^2=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},$$

$$\pi^3=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},$$

$$\pi^0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},$$

$$\pi^{-2}=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

二、循环

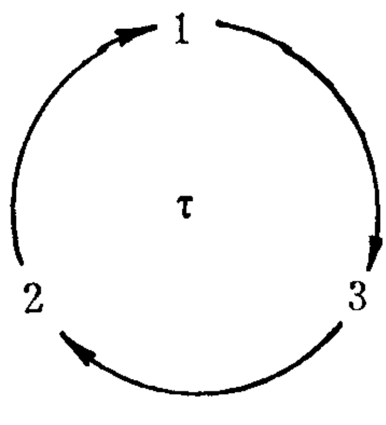


图 3—6

我们来看置换 $\tau=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$.

它把 1 变为 3，3 变为 2，2 又变为 1，是一个首尾相接的置换(如图 3—6)。

定义 2 形如

$$\begin{pmatrix}i_1&i_2&\cdots&i_k&i_{k+1}&\cdots&i_n\\i_2&i_3&\cdots&i_1&i_{k+1}&\cdots&i_n\end{pmatrix}$$

的置换，称为一个 k—循环，记为$(i_1i_2\cdots i_k)$。

这就是说，k—循环是一个特殊的置换，其中有 k 个元素循环置换($k\leqslant n$)，另外 $n-k$ 个元素不动。上面的置换 τ 是一个 3—循环。恒等变换被认为是一个 1—循环，记为(1)。置换如果是循环，则其不动元不再写入循环中。

一个循环的记号并不是唯一的，如上述 τ 可以写成(1 3 2)，也可以写成（3 2 1）或(2 1 3)，只要相连的次序不变，哪个元素开头都可以。

循环不仅写法简单，而且有许多重要性质：

性质 1 k—循环$(i_1i_2\cdots i_k)$是 k 阶元。

性质 2 $(i_1i_2\cdots i_k)^{-1}=(i_ki_{k-1}\cdots i_1)$。

性质 3 不相交(即无公共元素)的循环乘积的因子可以交换次序。

定理 1 任意 n 次置换 π 可以分解为若干不相交的循环的乘积。

证明：任取 i_1，如果$\pi(i_1)=i_1$，则(i_1)是一个循环。如果$\pi(i_1)\neq i_1$，设$\pi(i_1)=i_2$，又设$\pi(i_2)=i_3$，…。由于集合的有限性，上述过程不会无限继续下去，必然出现重复。设第一次出现的重复元素是i_k，$i_k=i_l$，i_l 是i_1，i_2，…，i_{k-1}中的一个。假若$i_l\neq i_1$，则由于$\pi(i_{l-1})=i_l=i_k=\pi(i_{k-1})$，得到$i_{l-1}=i_{k-1}$。说明 i_{k-1} 也是一个重复元素，与i_k 是第一个重复的元素这一假定矛盾。因而$i_k=i_1$，得到一个循环 $(i_1i_2\cdots i_k)$。如果$k<n$，再任取另外一个元素，例如 j_1，同样又得出一个循环$(j_1j_2\cdots j_h)$。这两个循环不会有共同的元素。如不然，设 $i_p=j_q$ 是公共元素，$1\leqslant p\leqslant k$，$1\leqslant q\leqslant h$，则

$$\pi^{p-1}(i_1)=i_p=j_q=\pi^{q-1}(j_1).$$

不妨设 $p\geq q$，则$\pi^{p-q}(i_1)=j_1$。因而 j_1 成为循环$(i_1i_2\cdots i_k)$中的元素，与 j_1的选取矛盾。如果上述两个循环之外，仍有元素，则继续这一过程，直至将$\{1, 2, \cdots, n\}$中元素全部包括为止。于是，显然有

$$\pi=(s_1s_2\cdots s_t)\cdots(j_1j_2\cdots j_h)(i_1i_2\cdots i_k)。$$

证毕

注意：置换分解为不相交循环乘积的时候，恒等置换(i)可以省略。

例1 将置换

$$\pi=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 3 & 1 & 2 & 5 & 7 & 8 & 4 & 6\end{pmatrix}$$

分解为不相交循环的乘积．并求π在S_8中的阶。

解：由于 $1\to3\to2\to1$，

$4\to5\to7\to4$，

$6\to8\to6$，

所以$\pi=(6\ \ 8)(4\ \ 5\ \ 7)(1\ \ 3\ \ 2)$。

$(1\ \ 3\ \ 2)$和$(4\ \ 5\ \ 7)$是3阶元素，$(6\ \ 8)$是2阶元素．设π的阶为 t，则由性质3

$$(1)=\pi^t=(6\ \ 8)^t(4\ \ 5\ \ 7)^t(1\ \ 3\ \ 2)^t。$$

由性质1，$3|t$，$2|t$，t是2，3的公倍数，即$6|t$。另一方面，$\pi^6=(1)$。因而 $t=6$。

上述结果加以推广，便是

性质4 设π_1，π_2，…，π_r是互不相交的循环，含元素个数分别是 k_1，k_2，…，k_r，则$\pi_r\cdots\pi_2\pi_1$的阶为$k_1, k_2, \cdots, k_r$的最小公倍数。

证明方法类似例1，请读者完成。

例 2 将置换

$\pi=(1\ \ 2)(4\ \ 7\ \ 8)(2\ \ 1)(7\ \ 2\ \ 8\ \ 1\ \ 5)(3\ \ 6)$

写成不相交的循环的乘积．

解：可以不必将 π 化为置换的一般形式，利用定理 1 证明中的方法，直接分解．

首先，写出一个左括号和 1，即

$$(1,$$

从右向左观察，看 1 变成什么？

右边第 2 循环将 1 变为 5，后面的循环不含 5，所以 $\pi(1)=5$．将 5 写在 1 的右边，即

$$(1\ \ 5,$$

再从右向左观察 $\pi(5)=?$

$$5\to 7\to 8,$$

即 $\pi(5)=8$，将 8 写在 5 的右边，成为

$$(1\ \ 5\ \ 8,$$

同样可以看出 $\pi(8)=1$，出现了循环．这时在 8 的右边加上右括号，即

$$(1\ \ 5\ \ 8).$$

循环外任取一个元素，例如 2，再用同样方法得到循环 $(2\ \ 4\ \ 7)$．

这时还剩下 3，6 两个，它们作成一个循环 $(3\ \ 6)$．

因而，$\pi=(3\ \ 6)(2\ \ 4\ \ 7)(1\ \ 5\ \ 8)$．

三、有限群的正则实现

上节凯莱定理，具体到有限群就是

定理 2 任何有限群与一个置换群同构．

例 3 写出与克莱茵四元群 B_4（见§3·1 例 4）同构的置换群。

解： 将 a，b，c，d 代之以 1，2，3，4. 构造集合 $\{1,2,3,4\}$ 的变换 σ_1，σ_2，σ_3，σ_4 如下：

$\sigma_1(1)=1\cdot1=1$，$\sigma_1(2)=1\cdot2=2$，$\sigma_1(3)=1\cdot3=3$，$\sigma_1(4)=1\cdot4=4$，即 $\sigma_1=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=(1)$.

$\sigma_2(1)=2\cdot1=2$，$\sigma_2(2)=2\cdot2=1$，$\sigma_2(3)=2\cdot3=4$，$\sigma_2(4)=2\cdot4=3$，即 $\sigma_2=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1\ \ 2)(3\ \ 4)$.

$\sigma_3(1)=3\cdot1=3$，$\sigma_3(2)=3\cdot2=4$，$\sigma_3(3)=3\cdot3=1$，$\sigma_3(4)=3\cdot4=2$，即 $\sigma_3=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ \ 3)(2\ \ 4)$.

$\sigma_4(1)=4\cdot1=4$，$\sigma_4(2)=4\cdot2=3$，$\sigma_4(3)=4\cdot3=2$，$\sigma_4(4)=4\cdot4=1$，即 $\sigma_4=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1\ \ 4)(2\ \ 3)$.

所以，这个置换群是$\{(1),(1\ \ 2)(3\ \ 4),(1\ \ 3)(2\ \ 4),(1\ \ 4)(2\ \ 3)\}$，它是 S_4 的一个子群，亦记为 B_4.

四、对换

定义 3 2—循环称为对换.

如$(1\ \ 3)$，$(2\ \ 5)$等都是对换.

定理 3 任何循环等于若干对换之积.

证明： 等式

$$(i_1i_2\cdots i_n)=(i_1i_n)\cdots(i_1i_3)(i_1i_2) \tag{1}$$

显然成立.

证毕

定理 4 任何置换等于若干对换之积。

证明：由定理 1 和定理 3 直接可得。

例 4 将置换 $\pi=(1\ \ 2\ \ 5)(3\ \ 4\ \ 6\ \ 7)$ 分解成对换乘积。

解：$(1\ \ 2\ \ 5)=(1\ \ 5)(1\ \ 2)$，

$(3\ \ 4\ \ 6\ \ 7)=(3\ \ 7)(3\ \ 6)(3\ \ 4)$，

所以 $\pi=(1\ \ 5)(1\ \ 2)(3\ \ 7)(3\ \ 6)(3\ \ 4)$。

置换分解成对换乘积时因子个数不是唯一的。如例 4 中置换 π 也可以写成：

$$\pi=(2\ \ 1)(2\ \ 5)(2\ \ 1)(1\ \ 2)(3\ \ 7)(1\ \ 3)(1\ \ 6)(1\ \ 3)(3\ \ 4)=(1\ \ 2)(2\ \ 5)(3\ \ 4)(4\ \ 6)(1\ \ 6)(1\ \ 7)(1\ \ 6)。$$

（还可有其他分解方式）这三种分解中，因子个数分别是 5，9，7，是奇数，π 绝不能分解成偶数个对换因子的乘积，一般地，我们有

定理 5 任意置换分解为对换乘积时，因子个数的奇偶性是不变的。

分析：先证对于恒等置换定理成立，然后借此推证一般的情况。

证明：设 $S=\{1,\ 2,\ \cdots,\ n\}$，$n\geqslant 2$。

设恒等置换 ε 有分解

$$\varepsilon=\tau_k\cdots\tau_2\tau_1, \tag{2}$$

其中 τ_i 是对换。下面证明 k 是偶数。

任取出现在 (2) 中的一个数字，设为 m。从右向左看，假设第一次出现 m 的因子是 $\tau_t(1\leqslant t\leqslant k)$，则 $t\neq k$（否则 $\varepsilon(m)\neq m$），即 τ_t 左面有因子 τ_{t+1}。这时，只能有以下四种情

况：

(1) $\tau_{t+1}=\tau_t$；

(2) $\tau_{t+1}\neq\tau_t$，但 τ_{t+1} 含 m；

(3) τ_{t+1} 不含 m，但与 τ_t 有公共元素；

(4) τ_{t+1} 与 τ_t 无公共元素.

这 4 种情况下，$\tau_{t+1}\tau_t$ 分别为：

$$(m\quad i)(m\quad i)=\varepsilon;$$

$$(m\quad j)(m\quad i)=(m\quad i\quad j)=(m\quad i)(i\quad j);$$

$$(i\quad j)(m\quad i)=(m\quad j\quad i)=(m\quad j)(i\quad j);$$

$$(j\quad k)(m\quad i)=(m\quad i)(j\quad k).$$

如果出现情况(1)，则(2)式消去一对对换.

如果出现其他情况，则 m 第一次出现的因子将在 (2)式中向左移一个位置.

继续做下去，由于 m 不能仅在(2)式的最后(左)的因子里出现，所以最终必然消去 m.

再另取 S 中的一个数字，类似地也可将其在(2) 式中消去. 于是，(2)式最后化为

$$\varepsilon=\varepsilon\cdot\varepsilon\cdots\varepsilon, \tag{3}$$

刚才的消去过程的每步，或者使(2)的因子同时去掉两个，或者个数不变，因而因子个数的奇偶性不变，最后，(3)式的对换因子个数是 0，为偶数，所以 k 与 0 同奇偶，即是偶数.

下面考查任意置换 π. 设 π 表为对换乘积时有两种方式：

$$\pi=\tau_r\cdots\tau_2\tau_1=\sigma_s\cdots\sigma_2\sigma_1.$$

由于每个对换与其逆相等、得到

$$\varepsilon=\pi\pi^{-1}=(\tau_r\cdots\tau_2\tau_1)(\sigma_s\cdots\sigma_2\sigma_1)^{-1}$$

$$= \tau_r \cdots \tau_2 \tau_1 \sigma_1^{-1} \sigma_2^{-1} \cdots \sigma_s^{-1}$$
$$= \tau_r \cdots \tau_2 \tau_1 \sigma_1 \sigma_2 \cdots \sigma_s.$$

由刚证得的结果，ε 的对换因子个数 $r+s$ 应为偶数，即 r 与 s 奇偶性相同。

证毕

定义 4 能表为偶数个对换乘积的置换，称为偶置换，否则称为奇置换。

由定理 5，一个置换的奇偶性是唯一确定的。

定理 6 偶置换之积或两奇置换之积都是偶置换；一个奇置换与一个偶置换之积是奇置换；偶置换之逆为偶置换；奇置换之逆为奇置换。

定理 7 任意 k—循环$(i_1 i_2 \cdots i_k)$的奇偶性与 k 的奇偶性刚好相反。

以上两定理由定义 4 和定理 3 容易证得，留作习题。

例 5 试判断$\pi=(1\ \ 2)(3\ \ 5\ \ 7)(4\ \ 6)$的奇偶性。

解：$(1\ \ 2)$，$(4\ \ 6)$都是奇置换，$(3\ \ 5\ \ 7)$是偶置换，故 π 是偶置换。

五、交错群

定理 8 全体 n 次偶置换作成置换群。

证明：由于偶置换之积以及偶置换之逆仍为偶置换，恒等置换是偶置换，所以全体 n 次偶置换作成对称群 S_n 的子群，即作成置换群。

证毕

定义 5 全体 n 次偶置换作成的置换群，称为 n 次交错群，记为 A_n。

交错群是一类重要的置换群．如

$$S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$$

中，(1)，$(1\ 2\ 3)$，$(1\ 3\ 2)$是全部偶置换．所以$A_3=\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$．

$|A_3|=3=\frac{1}{2}|S_3|$．一般地，我们有

定理 9 $|A_n|=\frac{1}{2}|S_n|=\frac{1}{2}n!$．$(n\geqslant 2)$

证明：设B_n是全体n次奇置换的集合．作A_n到B_n的映射σ：$\sigma(\tau)=(1\ 2)\tau$，$\tau\in A_n$．显然σ是一一映射．所以$A_n\sim B_n$，$|A_n|=|B_n|=\frac{|S_n|}{2}=\frac{n!}{2}$．

证毕

习 题 3·7

1．计算以下置换之积：

(1) $\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$；

(2) $\begin{pmatrix}1&2&3&4&5\\3&1&5&2&4\end{pmatrix}^{-1}\begin{pmatrix}1&2&3&4&5\\2&5&1&3&4\end{pmatrix}^2$．

2．将A_4中元素化为不相交循环的乘积．

3．将以下置换化为不相交循环的乘积：

(1) $(1\ 2\ 3)(4\ 5\ 6\ 8)(3\ 4)(5\ 2\ 6\ 1\ 8)(1\ 3\ 4)$；

(2) $(8\ 7\ 4\ 3\ 1\ 2)(5\ 6)(8\ 2\ 1\ 4\ 3)(1\ 2)$．

4．以下置换是置换群中的几阶元？

(1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 7 & 5 & 6 & 3 & 4 \end{pmatrix}$;

(2) $(1\ 4\ 3\ 2)(5\ 6)(7\ 8)$;

(3) $(1\ 2\ 3)(4\ 2\ 5\ 6\ 3)(3\ 2)$;

(4) $(1\ 2\ 3)^2(2\ 3\ 1)^{-1}(3\ 5\ 4\ 1)$。

5．将以下置换表为对换之积：

(1) $(1\ 2\ 3\ 5)(1\ 2\ 3)(4\ 3\ 2)(1\ 4)$;

(2) $(1\ 3\ 2)(1\ 2\ 3\ 5)(3\ 2\ 5)(1\ 2\ 3\ 4)$。

6．求证本节性质、定理 6 和定理 7．

7．找出 S_3 中由 $(1\ 3\ 2)$ 生成的子群．

8．求证：$\{(1\ 2),(2\ 3),\cdots,(n-1,\ n)\}$ 是 S_n 的生成系．

9．设 $\pi=(s_1\ s_2\cdots s_t)\cdots(j_1\ j_2\cdots j_h)(i_1\ i_2\cdots i_k)$，求证：$\pi^{-1}=(i_k\cdots i_2 i_1)(j_h\cdots j_2 j_1)\cdots(s_t\cdots s_2 s_1)$。

10．设 π 是一个 n 次置换，求证：

$$\pi(1\ 2\cdots r)\pi^{-1}=(\pi(1)\pi(2)\cdots\pi(r))。$$

§3·8　正规子群与商群

正规子群是一类重要的子群，由它可以产生出新的群——商群，这节就专门讨论这些问题．

一、正规子群

设 H 是群 G 的子群．H 在 G 中的所有左陪集，构成 G 的一种分类，同样，H 在 G 中的所有右陪集，也构成 G 的一种分类，这两种分类一般是不同的。如在三次对称群 S_3 中，

$$H=\{(1),(1\ \ 2)\}$$

是一个子群，它的左陪集、右陪集并不一致：

左陪集

$\{(1),(1\ \ 2)\},\{(1\ \ 3),(1\ \ 2\ \ 3)\},\{(2\ \ 3),(1\ \ 3\ \ 2)\}$

右陪集

$\{(1),(1\ \ 2)\},\{(1\ \ 3),(1\ \ 3\ \ 2)\},$
$\{(2\ \ 3),(1\ \ 2\ \ 3)\}.$

那末，有没有左、右陪集正好一致的子群呢？有的，如3次交错群 $A_3=\{(1),(1\ \ 2\ \ 3),(1\ \ 3\ \ 2)\}$ 就是 S_3 的这样一个子群. A_3 的左陪集和右陪集都是这样两个：

$\{(1),(1\ \ 2\ \ 3),(1\ \ 3\ \ 2)\},$
$\{(1\ \ 2),(1\ \ 3),(2\ \ 3)\}.$

定义 1 设 H 是群 G 的子群. 如果对于任意 $a\in G$，都有 $aH=Ha$，则称 H 是 G 的正规子群.

注意：$aH=Ha$ 是指集合相等，或者说群 G 中 $\{a\}$ 与 H 这两个集合的乘积可换，但不要理解为 a 与 H 的任意元素可换. 如上例中

$$(1\ \ 2)A_3=A_3(1\ \ 2),$$

但 $(1\ \ 2)(1\ \ 2\ \ 3)=(2\ \ 3)\neq(1\ \ 3)=(1\ \ 2\ \ 3)(1\ \ 2)$.

在上例中，H 不是 S_3 的正规子群，而 A_3 是 S_3 的正规子群.

任何群总有正规子群，因为显然平凡子群总是正规子群. 另外，对于可换群，所有子群自然都是正规子群.

判断一个子群是否正规子群，直接利用定义有时不甚方便，常用的判别定理是

定理 3 群G的子群N是正规子群的充要条件是：对任意的$g\in G$及$n\in N$，都有

$$gng^{-1}\in N. \tag{1}$$

证明： 如果N是正规子群，则$Ng=gN$对所有$g\in G$成立。任取$n\in N$，则$gn\in gN=Ng$，因而有$n_1\in N$，使$gn=n_1g$，从而$gng^{-1}=n_1gg^{-1}=n_1\in N$。

反之，如果条件(1)成立，任取$gn\in gN$，则$gng^{-1}\in N$。设$gng^{-1}=n_1$，则$gn=n_1g\in Ng$。因而$gN\subseteq Ng$。同样，任取$ng\in Ng$，由于$g^{-1}ng=g^{-1}n(g^{-1})^{-1}\in N$，因而有$n_2\in N$，使$g^{-1}ng=n_2$，$ng=gn_2\in gN$。所以$Ng\subseteq gN$。总之，$Ng=gN$，$N$是$G$的正规子群。

证毕

例 1 在群$M_n^*(\boldsymbol{R})$中(见§3·1例6)，由所有行列式等于1的n阶实方阵组成的集合N作成正规子群。

证明： 任取A，$B\in N$，即$|A|=|B|=1$，因而

$$|AB^{-1}|=|A|\cdot|B^{-1}|=|A|\cdot|B|^{-1}=1\cdot1=1.$$

即$AB^{-1}\in N$。由§3·3定理2，N是子群。

任取$A\in M_n^*(\boldsymbol{R})$和$B\in N$，则

$$|ABA^{-1}|=|A|\cdot|B|\cdot|A|^{-1}=|A|\cdot|A|^{-1}=1.$$

所以$ABA^{-1}\in N$·由定理3，N是正规子群。

二、群的中心

一个群中可以与任意元素交换的元素总是有的，如单位元就是一个，其他可能还有，这种元素组成群的重要子集。

定义 2 群G中与任意元素可换的全体元素组成的集合，称为群G的中心。

显然，可换群的中心与全群重合.

例 2　正方形对称群 D_4(§ 3·6 例 4)中，由乘法表可见，只有 $R_{2\pi}$、R_π 与任意元素可换，故中心 = $\{R_{2\pi}, R_\pi\}$。

显然，群的中心是所有元素正规化子之交，因而是子群，且显然是可换子群. 不仅如此，它还是正规子群. 事实上，任取 $c \in C$(群的中心)，$g \in G$，则

$$gcg^{-1} = gg^{-1}c = c \in C.$$

三、商群

正规子群产生的左、右陪集完全一样，所以，这时可以不加区分地称为陪集. 群 G 的正规子群 N 的所有陪集形成 G 的分类，因而产生了商集合，记为 G/N. 即

$$G/N = \{gN \mid g \in G\}.$$

注意：G/N 的元素是陪集，不是 G 的元素. 这时陪集已抽象为一种元素，不要再看作是 G 的子集了.

商集合 G/N 中规定法则：

$$aN \cdot bN = abN. \tag{2}$$

即规定 a 所在的陪集与 b 所在的陪集的乘积为 ab 所在的陪集.

定理 4　设 N 是群 G 的正规子群，则

(1) 法则(2)是 G/N 的代数运算；

(2) $\langle G/N, \cdot \rangle$ 是群.

分析：为证明法则(2)是代数运算，只须证明：如果 a_1 和 a 属同一陪集，b_1 和 b 属同一陪集，则 a_1b_1 与 ab 属同一陪集.

证明：(1) 如果 $a_1N = aN$，$b_1N = bN$，即有 $a_1 \in aN$，

$b_1 \in bN$,因而存在 $n_1, n_2 \in N$，使 $a_1 = an_1$，$b_1 = bn_2$，即 $a_1b_1 = an_1bn_2$。由于 N 是正规子群，所以 $n_1b \in bN = Nb$，因而存在 $n_3 \in N$，使 $n_1b = bn_3$. 这样一来，

$$a_1b_1 = a(bn_3)n_2 = (ab)(n_3n_2) \in abN.$$

所以 $a_1b_1N = abN$。

即法则(2)是 G/N 的代数运算，或说 $\langle G/N, \cdot \rangle$ 是群胚。

(2) 任取 $aN, bN, cN \in G/N$，则

$$(aN \cdot bN) \cdot cN = (abN) \cdot cN = [(ab) \cdot c]N,$$

$$aN \cdot (bN \cdot cN) = aN \cdot (bcN) = [a \cdot (bc)]N.$$

由于 $(ab)c = a(bc)$，故 $\langle G/N, \cdot \rangle$ 结合律成立.

$N = eN$ 是 $\langle G/N, \cdot \rangle$ 的单位元. 事实上，

$$eN \cdot aN = eaN = aN,$$

$$aN \cdot eN = aeN = aN.$$

$a^{-1}N$ 是 aN 的逆元. 事实上，

$$a^{-1}N \cdot aN = a^{-1}aN = eN,$$

$$aN \cdot a^{-1}N = aa^{-1}N = eN.$$

总之，$\langle G/N, \cdot \rangle$ 是群.

证毕

如果 H 是一个非正规子群，全体左(或右)陪集虽形成 G 的分类，因而可以作成商集合，但法则(2)不是代数运算.如 S_3 中，由 $H = \{(1), (1\ 2)\}$ 产生的左陪集中,有

$$(1\ 2\ 3)H = (1\ 3)H, (1\ 3\ 2)H = (2\ 3)H,$$

如按法则(2)，应有

$$(1\ 2\ 3)H \cdot (1\ 3\ 2)H = (1\ 3)H \cdot (2\ 3)H.$$

然而

$$(1\ 2\ 3)(1\ 3\ 2)H = (1)H = H,$$

$$(1\ 3)(2\ 3)H = (1\ 3\ 2)H.$$

$$H \neq (1\ \ 3\ \ 2)H.$$

出现矛盾．同样，它的右陪集的商集合，也不能形成群胚．

定义 3 由正规子群 $\langle N,\cdot\rangle$ 在群 $\langle G,\cdot\rangle$ 中的全体陪集按法则(2)作成的群，称为 G 关于 N 的商群，记为 $\langle G/N,\cdot\rangle$ 或 G/N．

注意：商群的乘法仍用原群中乘法的记号，但它们含义是不同的．

对于有限群 G，商群的阶是 N 在 G 中的指数，因而由拉格朗日定理，得到一个有趣的公式：

$$|G/N| = \frac{|G|}{|N|}. \tag{3}$$

例 3 在 $\langle \mathbf{Z},+\rangle$ 中，取一个固定的正整数 n，由 n 的所有倍数组成的集合

$$N = \{kn \mid k \in \mathbf{Z}\}$$

是一个子群，因为群是可换群，故 $\langle N,+\rangle$ 是一个正规子群．它决定的陪集共有 n 个：

$$N,\ 1+N,\ 2+N,\ \cdots,\ (n-1)+N.$$

它们组成的商群 $\langle \mathbf{Z}/N,+\rangle$ 即 $\langle \mathbf{Z}_n,+\rangle$．所以，以 n 为模的剩余类加群，就是整数加群关于 n 的倍数构成子群的商群．

例 4 在正方形对称群 D_4 中，其中心 $C=\{R_{2\pi},R_\pi\}$ 的商群 D_4/C 共含 4 个元素：

$$\{R_{2\pi},R_\pi\},\ \{R_{\frac{\pi}{2}},R_{\frac{3}{2}\pi}\},\ \{V,H\},\ \{D_1,D_2\}.$$

根据乘法的规定，可以得到商群的乘法表：

$\cdot$	$\{R_{2\pi}, R_{\pi}\}$	$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$	$\{V, H\}$	$\{D_1, D_2\}$
$\{R_{2\pi}, R_{\pi}\}$	$\{R_{2\pi}, R_{\pi}\}$	$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$	$\{V, H\}$	$\{D_1, D_2\}$
$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$	$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$	$\{R_{2\pi}, R_{\pi}\}$	$\{D_1, D_2\}$	$\{V, H\}$
$\{V, H\}$	$\{V, H\}$	$\{D_1, D_2\}$	$\{R_{2\pi}, R_{\pi}\}$	$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$
$\{D_1, D_2\}$	$\{D_1, D_2\}$	$\{V, H\}$	$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$	$\{R_{2\pi}, R_{\pi}\}$

下面，把商群的结构描述一下：

1．商群 G/N 是由群 G 和它的正规子群 N 所决定的一个新的群；

2．商群的元素是 N 在 G 中的所有陪集；

3．商群的单位元是正规子群 N．N 是唯一成为子群的陪集，其他陪集都不是子群；

4．商群中元素（陪集）的逆元，就是这个陪集中任一元素的逆元所在的陪集；

5．商群中两元素（两陪集）的积是这两个陪集中任意两元素之积所在的陪集．

习　题　3·8

1．求证：群的指数为 2 的子群是正规子群．

2．求证：A_n 是 S_n 的正规子群．

3．求证：$B_4=\{(1),(1\ \ 2)(3\ \ 4),(1\ \ 3)(2\ \ 4),(1\ \ 4)(2\ \ 3)\}$ 作成 A_4 的正规子群．

4．求证：两正规子群的交或积都是正规子群．

5．群的正规子群的正规子群是否正规子群？举例说明．

6. 一个群中如果某阶的子群只有一个，那末这个子群是正规子群. 试证明之.

7. 设H和N分别是群G的子群和正规子群，求证：$H\cap N$是H的正规子群，HN是G的子群.

8. 设G是群，规定$a\sim b\Longleftrightarrow$存在$g\in G$，使$a=g^{-1}bg$. 求证：$\sim$是$G$的等价关系.

9. 写出S_3的所有正规子群和S_3的中心.

10. 求证：循环群的商群也是循环群.

11. 求证：群中心的子群是原群的正规子群.

12. 写出D_4的所有正规子群.

13. 设N为群G的子群，求证：N是正规子群$\Longleftrightarrow$对所有$g\in G$，$gNg^{-1}=N$.

§3·9 群的同态

群是特殊的半群，半群同态的性质（§2·5）群同态自然也具备，如单位元的同态象是单位元，元素逆元的同态象是这个元素象的逆元，等等. 但群同态还有自己的特点.

一、同态的性质

设φ是群G到群H的同态，即对于$a,b\in G$，总有$\varphi(ab)=\varphi(a)\varphi(b)$. 在$\varphi$作用下，$e_H$的原象集称为$\varphi$的核，记为$K_\phi$. 即

$$K_\phi=\{g\in G\mid \varphi(g)=e_H\}=\varphi^{-1}[e_H].$$

定理1 （1）K_ϕ是G的正规子群；（2）当且仅当$K_\phi=\{e_G\}$时，φ为单同态；（3）G中两个元素当且仅当属于K_ϕ

的同一陪集时，有相同的象．即 $\varphi[G]$中任一元素的原象集是一个陪集．

证明：(1) $e_G \in K_\varphi \neq \phi$．任取 a，$b \in K_\varphi$．由于 φ 是同态，故有

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = e_H\varphi(b)^{-1} = e_H e_H^{-1} = e_H.$$

即 $ab^{-1} \in K_\varphi$，K_φ 是 G 的子群．任取 $k \in K_\varphi$，$a \in G$，则

$$\begin{aligned}\varphi(aka^{-1}) &= \varphi(a)\varphi(k)\varphi(a^{-1}) = \varphi(a)e_H\varphi(a)^{-1}\\ &= \varphi(a)\varphi(a)^{-1} = e_H.\end{aligned}$$

即 $aka^{-1} \in K_\varphi$．由§3·8 定理 3，k_φ 是 G 的正规子群．

(2) 如果 φ 是单同态，则 e_H 的原象是唯一的，$K_\varphi = \{e_G\}$．反之，如果 $K_\varphi = \{e_G\}$，这时假定 a 和 b 的象相同，即 $\varphi(a) = \varphi(b)$，$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H$．因而 $ab^{-1} \in K_\varphi = \{e_G\}$，$ab^{-1} = e_G$，$a = b$，$\varphi$ 为单同态．

(3) 如果 $\varphi(a) = \varphi(b)$，则 $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = e_H$，故 $a^{-1}b \in K_\varphi$．由§3·4，a 与 b 同属 K_φ 的一个陪集．反之，如果 a 与 b 同属 K_φ 的一个陪集，则 $a^{-1}b \in K_\varphi$，$e_H = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b)$，得 $\varphi(a) = \varphi(b)$．

证毕

定理 2 $\varphi[G]$是 H 的子群．

证明：$\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi[G]$．由子群的判别定理，$\varphi[G]$是 H 的子群．

证毕

二、同态基本定理

例 1 设有$\langle \mathbf{R}_2, + \rangle$到$\langle \mathbf{R}, + \rangle$的映射 φ：

$$\varphi((a,b)) = a.\ (如图 3—7)$$

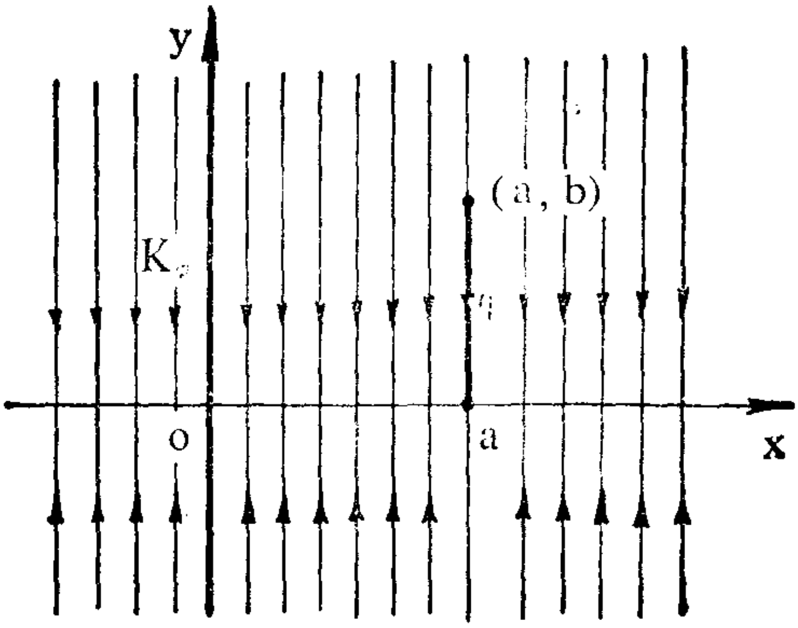


图 3—7

求证：(1) φ 是满同态；(2) $\boldsymbol{R}_2/K_\varphi \cong \boldsymbol{R}$。

证明：φ 实际上是平面到横轴的投影。

(1) 任取(a,b)，$(c,d) \in \boldsymbol{R}_2$，则

$$\varphi[(a,b)+(c,d)]=\varphi(a+c,b+d)=a+c;$$

而 $\varphi(a,b)+\varphi(c,d)=a+c$，所以 φ是同态。φ 为满射是显然的。

(2) $\langle \boldsymbol{R},+\rangle$的单位元是 0，象为 0 的元素是集合 $K_\varphi=\{(0,y)\mid y\in\boldsymbol{R}\}$，即 y 轴上的全部点。商群 $\boldsymbol{R}_2/K_\varphi$ 是全体陪集的集合，每个陪集形如：

$$(a,b)+K_\varphi=(a,b)+\{(0,y)\mid y\in\boldsymbol{R}\}$$
$$=\{(a,y)\mid y\in\boldsymbol{R}\}.$$

即平行于 y 轴的直线。$\boldsymbol{R}_2/K_\varphi$ 是竖直直线族。

每个陪集（这里是直线）中的所有元素经 φ 都映射为一个共同的元素（即 x 轴上的投影）。这样，就决定了商群 $\boldsymbol{R}_2/K_\varphi$ 到 $\boldsymbol{R}$ 的对应，将其记为 $\bar{\varphi}$。即

$$\bar{\varphi}((a,b)+K_\varphi)=a_\circ \qquad (1)$$

同一陪集中元素(x,y)的x都是一样的，所以(1)式的规定与陪集的代表元(a,b)的选取无关，即$\bar{\varphi}$是$\boldsymbol{R}_2/K_\varphi$到$\boldsymbol{R}$的映射.

$\bar{\varphi}$是同态．事实上，

$$\begin{aligned}&\bar{\varphi}((a,b)+K_\varphi)+\bar{\varphi}((c,d)+K_\varphi)\\&=a+c\\&=\bar{\varphi}((a+c,b+d)+K_\varphi)\\&=\bar{\varphi}(((a,b)+K_\varphi)+((c,d)+K_\varphi)).\end{aligned}$$

$\bar{\varphi}$是单射．事实上，如果$(a,b)+K_\varphi\neq(c,d)+K_\varphi$，由上所述，应有

$$\{(a,y)\,|\,y\in\boldsymbol{R}\}\neq\{(c,y)\,|\,y\in\boldsymbol{R}\}.$$

因而，有$a\neq c$,即经$\bar{\varphi}$映射的象也不同.

另外，$\bar{\varphi}$显然是满射，总之，$\bar{\varphi}$是同构映射.

$$\boldsymbol{R}_2/K_\varphi\cong\boldsymbol{R}_\circ$$

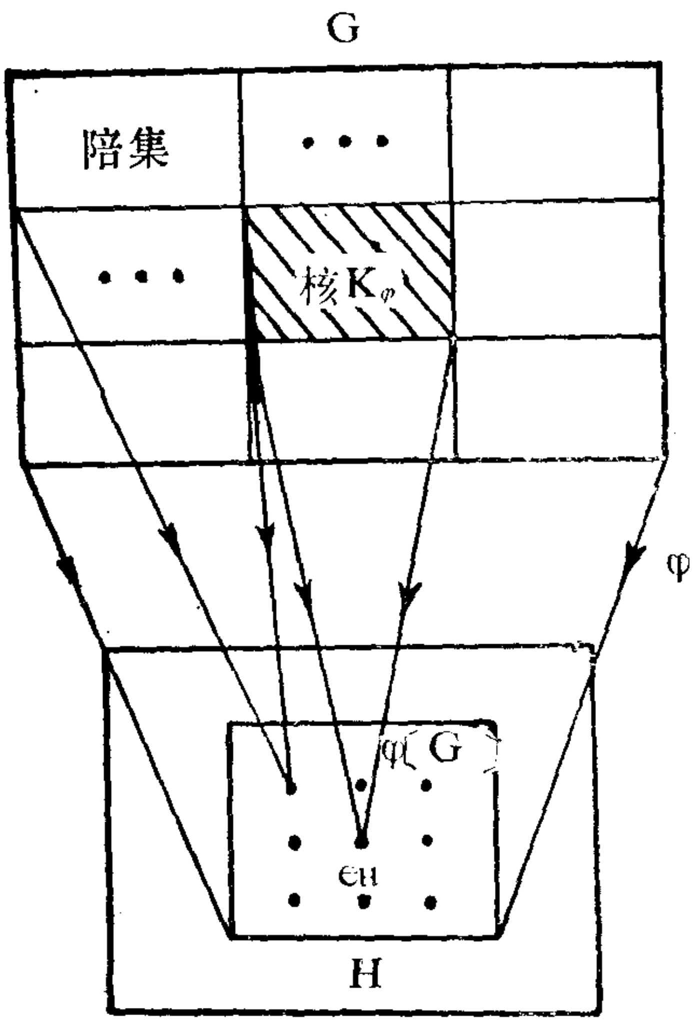


图 3—8

这个例子形象地说明了由群同态φ得到商群同构$\bar{\varphi}$的过程，方法具有一般性．对于群的同态φ，核K_φ中所

有元素映为一个元素 e_H，K_φ 的每一陪集的元素也只映为一个元素．因而，K_φ 的陪集的集合就与 φ 的象集 $\varphi[G]$之间一一对应起来，这是一个同构，于是 G/K_φ 与 $\varphi[G]$同构（如示意图 3—8)．这就是下述著名的"同态基本定理"的基本思想．

定理 3 设 φ 是群 G 到群 H 的同态，则

$$G/K_\varphi \cong \varphi[G].$$

证明：由定理 1 、 2 ，K_φ 是正规子群，$\varphi[G]$ 作成 H 的子群，从而存在商群 G/K_φ。考虑由 G/K_φ 到 $\varphi[G]$ 的对应法则 $\bar{\varphi}$：

$$\bar{\varphi}(gK_\varphi) = \varphi(g). \tag{2}$$

即 K_φ 的任意陪集对应其中任一元素在 φ 下的象．

$\bar{\varphi}$ 是映射．事实上，如果 g_1，g_2 同属一个陪集，即 $g_1^{-1}g_2 \in K_\varphi$，这时，

$$e_H = \varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2),$$

即 $\varphi(g_1) = \varphi(g_2)$．即法则(2)与陪集中的代表元选取无关．

$\bar{\varphi}$ 是满射．事实上，任取 $h \in \varphi[G]$，存在 $g \in G$，使 $h = \varphi(g)$，因而 $\bar{\varphi}(gK_\varphi) = \varphi(g) = h$．

$\bar{\varphi}$ 是单射．事实上，如果 $g_1K_\varphi \neq g_2K_\varphi$，则 g_1, g_2 不在同一陪集里，因而 $g_1^{-1}g_2 \notin K_\varphi$．即 $\varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2) \neq e_H$，$\varphi(g_1) \neq \varphi(g_2)$，

$$\bar{\varphi}(g_1K_\varphi) \neq \bar{\varphi}(g_2K_\varphi).$$

$\bar{\varphi}$是同态映射．事实上，

$\bar{\varphi}(g_1K_\varphi \cdot g_2K_\varphi) = \bar{\varphi}((g_1g_2)K_\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \bar{\varphi}(g_1K_\varphi)\bar{\varphi}(g_2K_\varphi)$．

总之，$\bar{\varphi}$ 是 G/K_φ 到 $\varphi[G]$的同构映射，即

$$G/K_\varphi \cong \varphi[G].$$

证毕

推论 1 如果 φ 是群 G 到 H 的满同态，则

$$G/K_\varphi \cong H.$$

推论 2 如果 G 是有限群，G 与 H 同态，则 H 也是有限群，且 $|H|$ 是 $|G|$ 的因子。

证明：由推论 1，$G/K_\varphi \cong H$。根据上节公式（3），$|H| = |G/K_\varphi| = \frac{|G|}{|K_\varphi|}$，故 $|H| \mid |G|$。

证毕

上面定理说明由同态可以决定正规子群（同态核），继而生成商群。反之，商群，也可以决定同态。

定理 4 设 G/N 是一个商群，则 G 与 G/N 同态。

证明：G/N 的元素是 G 关于 N 的陪集，陪集是 G 的分类，因而 G 中每个元素在且仅在一个陪集。让 G 的每个元素对应自己所在的陪集。即规定：$\varphi(g) = gN$。显然 φ 是满射。另外，由陪集乘法法则，

$$\varphi(g_1g_2) = (g_1g_2)N = g_1N \cdot g_2N = \varphi(g_1)\varphi(g_2).$$

得知 φ 是满同态，即 G 与 G/N 同态。

证毕

定理 4 中，由 G 到 G/N 的同态映射，称为自然同态。

综合上述，我们看到，一方面群同态于自己的商群，另一方面，群的同态象总与一个商群同构。这就是说，在同构的意义下，可以认为一个群的同态象是且仅是自己的商群。

一个群如有正规子群，就决定一个商群，因而就出现一个自然同态；一个群如有商群（当然也就有正规子群），因而有一个自然同态，这个正规子群就是自然同态的核。反之，如

果有了群同态，其同态核就是一个正规子群，于是决定一个商群。总之，正规子群、商群和同态三者只要有其一，就有另外两方面。

例2 考虑6阶循环群 $C_6=\{e,a,a^2,\cdots,a^5\}$ 的变换 φ：

$$\varphi(e)=\varphi(a^2)=\varphi(a^4)=e,$$
$$\varphi(a)=\varphi(a^3)=\varphi(a^5)=a^3.$$

则 φ 是自同态。

事实上，任取 a^k，$a^l\in C_6$，则

$$\varphi(a^ka^l)=\varphi(a^{k+l})=\begin{cases}e, & k+l\text{ 是偶数；}\\ a^3, & k+l\text{ 是奇数。}\end{cases}$$

$$\varphi(a^k)\varphi(a^l)=\begin{cases}e\cdot e=e, & k\text{ 和 }l\text{ 是偶数；}\\ e\cdot a^3=a^3, & k\text{ 是偶数，}l\text{ 是奇数；}\\ a\cdot e=a^3, & k\text{ 是奇数，}l\text{ 是偶数；}\\ a^3\cdot a^3=e, & k\text{ 和 }l\text{ 是奇数。}\end{cases}$$

$$=\begin{cases}e, & k+l\text{ 是偶数；}\\ a^3, & k+l\text{ 是奇数。}\end{cases}$$

易见

$$\varphi[C_6]=\{e,\ a^3\}=\langle a^3\rangle,$$
$$K_\varphi=\{e,a^2,a^4\}=\langle a^2\rangle.$$

因而 $C_6/\langle a^2\rangle\cong\langle a^3\rangle$。

例3 设 W 为全体模为1的复数集，即

$$W=\{\cos\theta+i\sin\theta\,|\,\theta\in\boldsymbol{R}\}.$$

求证：(1) $\langle W,\cdot\rangle$ 是群；

(2) $\langle\boldsymbol{R}/\boldsymbol{Z},+\rangle\cong\langle W,\cdot\rangle$。

证明：作 $\boldsymbol{R}$ 到 $\boldsymbol{C}^*$ 的映射 f：

$$f(x)=\cos 2\pi x+i\sin 2\pi x.$$

显然$|f(x)|\equiv 1$.

反之，如果$z=\cos y+i\sin y$，取$x=\dfrac{y}{2\pi}$，则$z=\cos 2\pi x+i\sin 2\pi x$。所以，映射$f$下$\boldsymbol{R}$的象集是模为1的复数集$W$。

f是同态。事实上，

$$
\begin{aligned}
f(x+y)&=\cos 2\pi(x+y)+i\sin(x+y)\\
&=(\cos 2\pi x+i\sin 2\pi x)(\cos 2\pi y+i\sin 2\pi y)\\
&=f(x)f(y).
\end{aligned}
$$

根据定理2，$\boldsymbol{R}$的同态象W是群。($\langle W,\cdot\rangle$是群也可直接证明)。

$$
\begin{aligned}
\boldsymbol{K}_f&=\{x\in\boldsymbol{R}\,|\cos 2\pi x+i\sin 2\pi x=1\}\\
&=\{x\in\boldsymbol{R}\,|\cos 2\pi x=1\}=\boldsymbol{Z}.
\end{aligned}
$$

由同态基本定理，$\langle\boldsymbol{R}/\boldsymbol{Z},+\rangle\cong\langle W,\cdot\rangle$。

例4　实n维向量空间$\boldsymbol{R}_n$，可以看作向量加群。设A是一个实n阶方阵，A决定$\langle\boldsymbol{R}_n,+\rangle$的一个变换$\varphi$：$\varphi(X)=AX$，其中$X$为实$n$维列向量。

易证φ是$\boldsymbol{R}_n$的自同态。其核K_φ是齐次方程组$AX=0$的解集合(提醒一句：0是$\boldsymbol{R}_n$的单位元)。显然，象集$\varphi[\boldsymbol{R}_n]=\{Y\,|\,Y=AX,\ X\in\boldsymbol{R}_n\}=\{Y\,|\,\text{方程组 }AX=Y\text{ 有解}\}$。

对于$b\in\varphi[\boldsymbol{R}_n]$，其原象集

$$\varphi^{-1}[b]=\{X\,|\,AX=b,\ X\in\boldsymbol{R}_n\},$$

即方程组$AX=b$的解集合。由定理1，$\varphi^{-1}[b]$是K_φ的一个陪集，即$\varphi^{-1}[b]=X_0+K_\varphi$，其中$X_0$是$\varphi^{-1}[b]$的固定元素，即方程组$AX=b$的特解。这一事实说明非齐次方程组的解集合是它的一个特解与对应齐次方程组(常称为导出方程组)解集

合的和．这与线性代数中学过的知识是一致的（如图 3—9）．

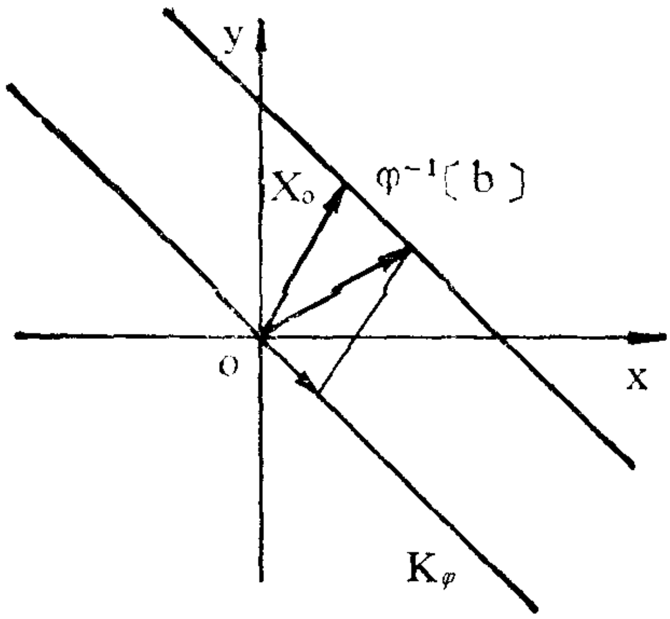


图 3—9

习 题 3·9

1．设群 G 与 $\bar{G}$ 同态，a 是 G 中有限阶元素，求证：a 的象也是有限阶的，其阶为 a 的阶的因子．

2．下列对应法则哪些是群同态？若是，试写出核与象集：

（1）$\langle \mathbf{Z}, +\rangle \to \langle \mathbf{R}, +\rangle$，$\varphi(n) = |n|$；

（2）$\langle \mathbf{R}^*, \cdot\rangle \to \langle \mathbf{R}^*, \cdot\rangle$，$\varphi(x) = |x|$；

（3）$\langle \mathbf{Z}, +\rangle \to \langle \mathbf{Z}_n, +\rangle$，$\varphi(x) = [x]$；

（4）$\langle \mathbf{Z}_8, +\rangle \to \langle \mathbf{Z}_2, +\rangle$，$\varphi([n]) = \begin{cases}[1], & n \text{ 是奇数}, \\ [0], & n \text{ 是偶数}; \end{cases}$

（5）$\langle \mathbf{Z}_7, +\rangle \to \langle \mathbf{Z}_2, +\rangle$，$\varphi([n])$ 规定同上．

3．让 n 次偶置换都对应 1，奇置换都对应 -1，求证这时 S_n 与 $\langle\{-1, 1\}, \cdot\rangle$ 同态．核是什么？

4．求证：C_n 与 C_m 同态当且仅当 $m|n$．

5. 设G是群，$a \in G$，规定 $\boldsymbol{Z}$ 到G的映射 φ 为：$\varphi(n)=a^n$。求证 φ 是同态，确定其核与象集。

6. 求证：$\langle \boldsymbol{C}^*/W,\cdot\rangle \cong \langle \boldsymbol{R}^+,\cdot\rangle$（见例 3）。

§3·10 同构定理

这一节是上节的继续，讨论同态下子群之间的关系。

一、子群的对应

定理 1 设 φ 是群G到群H的满同态，则

(1) G的子群的象集是H的子群；

(2) G的正规子群的象集是H的正规子群；

(3) H的子群的原象集是G的子群；

(4) H的正规子群的原象集是G的正规子群。

证明：(1) 设 G_1 是G的子群，$\varphi[G_1]=H_1\neq\phi$，任取 $h_1,h_2\in H_1$，则有 $g_1,g_2\in G_1$，使 $h_1=\varphi(g_1)$，$h_2=\varphi(g_2)$。因而 $h_1h_2^{-1}=\varphi(g_1)\varphi(g_2)^{-1}=\varphi(g_1g_2^{-1})$。$G_1$ 是子群，故$g_1g_2^{-1}\in G_1$，从而 $h_1h_2^{-1}\in H_1$，H_1 是子群。

(2) 设 G_2 是G的正规子群，$\varphi[G_2]=H_2$。由 (1)，H_2 是子群。另一方面，任取 $h_1\in H$，$h_2\in H_2$，则有 $g_1\in G$，$g_2\in G_2$ 使$\varphi(g_1)=h_1$，$\varphi(g_2)=h_2$。于是 $\varphi(g_1g_2g_1^{-1})=\varphi(g_1)\varphi(g_2)\cdot\varphi(g_1)^{-1}=h_1h_2h_1^{-1}$。$G_2$ 是正规子群，由 §3·8 定理 3，$g_1g_2g_1^{-1}\in G_2$，即 $h_1h_2h_1^{-1}\in H_2$。从而H_2是正规子群。

(3) 设 H_1 是 H 的子群，G_1 是 H_1 的原象集，即 $G_1=\varphi^{-1}[H_1]\neq\phi$。任取 $g_1,g_2\in G_1$，则

$$\varphi(g_1g_2^{-1})=\varphi(g_1)\varphi(g_2)_1^{-1}\in \mathrm{H}_1,$$

故 $g_1g_2^{-1}\in G_1$，G_1 是子群。

(4) 设 H_2 是H的正规子群,G_2 是H_2 的原象集．由 (3)，G_2 是G 的子群．另一方面，任取 $g_1\in G$，$g_2\in G_2$，则

$$\varphi(g_1g_2g_1^{-1})=\varphi(g_1)\varphi(g_2)\varphi(g_1)^{-1}\in H_2.$$

因而 $g_1g_2g_1^{-1}\in G_2$，G_2 是正规子群．

证毕

$H\to\varphi[H]$的对应显然保持子群的包含关系，但并非一一对应．如设 G_1 和 G_2 是 φ 的同态核 K_φ 的不同子群时，显然 $\varphi[G_1]=\varphi[G_2]=\{e_H\}$．然而 G 中一切包含核 K_φ 的子群却与H 的全体子群之间有一一对应．事实上，若 G_1 和 G_2 是G 中包含 K_φ 的不同子群，不妨设 $g_1\in G_1\backslash G_2$，则 $\varphi(g_1)\overline{\in}\varphi[G_2]$，因为否则必有 $g_2\in G_2$，使 $\varphi(g_1)=\varphi(g_2)$，因而 $\varphi(g_1g_2^{-1})=e_H$，$g_1g_2^{-1}\in K_\varphi$． 由于 $g_2\in G_2$，$K_\varphi\subseteq G_2$，推得 $g_1\in G_2$，矛盾．所以 $\varphi[G_1]\neq\varphi[G_2]$．另一方面，任取$H$ 的子群 H_1，$\varphi^{-1}[H_1]$ 显然是包含 K_φ 的子群，$\varphi\left[\varphi^{-1}[H_1]\right]=H_1$．显然，在上述子群的一一对应下，正规子群也是一一对应的．

现在假定N是G的正规子群，$H=G/N$．G与H同态，同态映射为自然同态：$\varphi(g)=gN$．其同态核为N．由定理1和上面的讨论不难得到

推论 1 设N是群G的正规子群，则G/N的子群形如 $H/N=\{hN\mid h\in H\}$（H 是G的含N的子群)，正规子群形如 $H_1/N=\{h_1N\mid h_1\in H_1\}$（$H_1$ 是G 的含 N 的正规子群)，同时，G 的全体含N 的子群(或正规子群)与G/N 的全体子群(或正规子群)之间有一一对应．

二、同构定理

现在我们把同态基本定理加以推广.

设群G与群H同态，由同态基本定理，$G/N\cong H$, H也可以看成商群$H/\{e\}$，这里N是同态核，e是H的单位元，即N是e的原象集. $\{e\}$是H的特殊的正规子群. 如果H_1是H的任意正规子群，G_1是H_1的原象集，是否有$G/G_1\cong H/H_1$呢?

定理 2（第一同构定理） 设群G与群H同态，H_1是H的正规子群，G_1是H_1的原象集，则

$$G/G_1\cong H/H_1.$$

分析：构造G到H/H_1的满同态，其核为G_1，然后利用同态基本定理.

证明：由定理1，G_1是G的正规子群. 设G到H的同态是φ. 对任意的$g\in G$，规定G到H/H_1的映射σ如下：

$$\sigma(g)=\varphi(g)H_1.$$

就是说，$\sigma(g)$是g在φ下的象$\varphi(g)$所在的陪集.

σ是满射. 事实上，任取$hH_1\in H/H_1$，由于φ是满射，故存在$g\in G$，使$\varphi(g)=h$，因而$\sigma(g)=\varphi(g)H_1=hH_1$.

σ是同态. 事实上，任取g_1，$g_2\in G$，则

$$\sigma(g_1g_2)=\varphi(g_1g_2)H_1=(\varphi(g_1)\varphi(g_2))H_1$$
$$=\varphi(g_1)H_1\cdot\varphi(g_2)H_1=\sigma(g_1)\sigma(g_2).$$

因而，σ是满同态.

G_1是σ的核. 事实上，由于H_1是H/H_1的单位元，H_1的σ原象集是由在φ下其象属于H_1的那些元素组成，即$\varphi^{-1}[H_1]$. 所以$\sigma^{-1}[H_1]=G_1$.

由同态基本定理，$G/G_1 \cong H/H_1$。

证毕

例 1　设G是 12 阶循环群$\{e, a, a^2, \cdots, a^{11}\}$，$H$是 6 阶循环群$\{\bar{e}, b, b^2, \cdots, b^5\}$。规定

$$\sigma(e)=\sigma(a^6)=\bar{e}, \qquad \sigma(a)=\sigma(a^7)=b,$$
$$\sigma(a^2)=\sigma(a^8)=b^2, \qquad \sigma(a^3)=\sigma(a^9)=b^3,$$
$$\sigma(a^4)=\sigma(a^{10})=b^4, \qquad \sigma(a^5)=\sigma(a^{11})=b^5.$$

易见，σ是G到H的满同态。$\{\bar{e}, b^3\}=\langle b^3\rangle$是$H$的子群，也是正规子群，其原象集是$\{e, a^3, a^6, a^9\}=\langle a^3\rangle$。由第一同构定理，

$$G/\langle a^3\rangle \cong H/\langle b^3\rangle.$$

第一同构定理讲的是两个同态群的商群之间的一个同构关系。对于一个群来说，它的两个子群的积与交之间也可以建立同构。让我们先介绍正规子群的几个性质。

引理 1　设N是群G的正规子群，H是G的子群，则

(1) HN是G的子群；

(2) N是HN的正规子群；

(3) $H\cap N$是H的正规子群。

证明：(1) $HN=\{hN \mid h\in H\}$。N是正规子群，故$hN=Nh$。因而$HN=\{Nh \mid h\in H\}=NH$。由§3·3 定理 8，HN是G的子群。

(2) N是HN的子群，又因$gN=Ng$对所有$g\in G$成立，自然对所有$g\in HN$也成立。所以N是HN的正规子群。

(3) $H\cap N$是H的子群。另外，对于任意的$h\in H$和$n\in H\cap N$，积$hnh^{-1}\in H$。同时，由于N是正规子群，故$hnh^{-1}\in N$。因而$hnh^{-1}\in H\cap N$。$H\cap N$是H的正规子群。

证毕

定理 3（第二同构定理） 设N是群G的正规子群，H是G的子群，则

$$HN/N\cong H/H\cap N.$$

注意：由引理 1，上述两个商群都是有意义的.

证明：由§3·9 定理 4，G 与 G/N 同态. 设φ是对应的自然同态，其同态核是子群N. 设$\varphi[H]=\bar{H}\subseteq G/N$，$\bar{H}$由$H$的元素所在的陪集组成，即$\bar{H}=\{hN|h\in H\}$. 由定理1，$\bar{H}$是$G/N$的子群. H与$\bar{H}$同态，其核为H中属于N的元素组成的集合，即$H\cap N$. 由同态基本定理，$\bar{H}\cong H/H\cap N$.

另一方面，$\bar{H}$在φ下的原象集$\varphi^{-1}[\bar{H}]$，显然是$\bar{H}$中所有陪集（即$\bar{H}$的元素）作为G的子集的并集. 即

$$\varphi^{-1}[\bar{H}]=\bigcup_{h\in H}hN=\{hn|h\in H,\ n\in N\}=HN.$$

这样，就有$\varphi[HN]=\bar{H}$. HN与$\bar{H}$看作独立的群是同态的，其同态核是N. 即$HN/N\cong\bar{H}$.

由于同构的传递性，故

$$HN/N\cong H/H\cap N.$$

证毕

例 2 设G是一个n次置换群. G中含有奇置换.求证：G中的偶置换组成一个指数为 2 的正规子群.

证明：G中含有偶置换(1).故G里面的偶置换集$H\neq\phi$. 偶置换之逆是偶置换，两偶置换之积也是偶置换，故H作成G的子群.

A_n是S_n的指数为 2 的正规子群，这是因为任取$\sigma\in A_n,\tau\in S_n,\tau\sigma\tau^{-1}$总是一个偶置换，$|A_n|=\frac{1}{2}|S_n|$. 另

外，设π为G中的奇置换，故$GA_n \supseteq \pi A_n \cup (1)A_n = S_n$。即$S_n = GA_n$。其次，显然$G \cap A_n = H$。由定理2，$G \cap A_n$是$G$的正规子群。据第二同构定理，$GA_n/A_n \cong G/G \cap A_n$，即$S_n/A_n \cong G/H$。而$(S_n:A_n)=2$，故$(G:H)=2$。

*下面介绍群的第三同构定理（Zassenhaus 定理），它讨论一个群中四个子群的关系（证明从略）。

定理4（第三同构定理） 设K，L，K'，L'是群G的子群，K'和L'分别是K和L的正规子群，则$K'(K \cap L')$是$K'(K \cap L)$的正规子群，$L'(L \cap K')$是$L'(L \cap K)$的正规子群，$(K' \cap L)(K \cap L')$是$K \cap L$的正规子群，且

$$K'(K \cap L)/K'(K \cap L') \cong (K \cap L)/(K' \cap L)(K \cap L') \cong L'(L \cap K)/L'(L \cap K').$$

由这一定理可推得第二同构定理，如取$K=H$，$K'=\{e\}$，$L=G$，$L'=N$，即得$H/H \cap N \cong NH/N$。有趣的是，由第二同构定理也可推得此定理（见习题3·10第6题）。

习　题　3·10

1．设群G与群$\bar{G}$同态，同态映射为φ，H是G的子群。求证：$\varphi^{-1}[\varphi[H]]$与$\varphi[H]$同态。

2．设N是G的正规子群，H是G的子群，$H \cap N = \{e\}$，则$HN/N \cong H$。试证明之。

*3．设H和K是群G的正规子群，$K \subseteq H$，求证：$G/H \cong G/K/H/K$。

4．利用第二同构定理证明：$S_4/B_4 \cong S_3$。其中$B_4 = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$。

5．设G为无限循环群$\langle a \rangle$，n，m是正整数。试用第二同

构定理证明：$\langle a^d\rangle/\langle a^n\rangle\cong\langle a^m\rangle/\langle a^l\rangle$。其中 $d=(m, n), l=[m, n]$。

*6. 试由群的第二同构定理推证第三同构定理。

§3·11 群的自同态与自同构

这一节讨论群到自身的同态与同构，即自同态与自同构。

一、从自同态到自同构

任何群总有自同态，因为恒等变换以及变全体元素为单位元的变换都是自同态。

自同构是特殊的自同态。恒等变换是自同构。

群 G 作为一个集合，它的全体变换作成半群 $\boldsymbol{S}(G)$，而其全体一一变换作成群 $\boldsymbol{G}(G)$（见§3·6）。设群 G 的全体自同态构成的集合为 $\boldsymbol{E}(G)$，全体自同构构成的集合为 $\boldsymbol{A}(G)$。显然，$\boldsymbol{E}(G)\subseteq\boldsymbol{S}(G)$，$\boldsymbol{A}(G)\subseteq\boldsymbol{G}(G)$，$\boldsymbol{A}(G)\subseteq\boldsymbol{E}(G)$。

定理1 设 G 是群，按照集合 G 中变换的乘法，$\boldsymbol{E}(G)$ 作成半群，$\boldsymbol{A}(G)$ 作成群，它们分别是 $\boldsymbol{S}(A)$ 的子半群和 $\boldsymbol{G}(G)$ 的子群，且 $\boldsymbol{A}(G)=\boldsymbol{E}(G)\cap\boldsymbol{G}(G)$。

证明：设 σ, τ 是 G 的自同态。任取 $a,b\in G$，则

$$\sigma\tau(ab)=\sigma(\tau(ab)=\sigma(\tau(a)\tau(b))=\sigma\tau(a)\cdot\sigma\tau(b).$$

因而 $\sigma\tau\in\boldsymbol{E}(G)$。$\boldsymbol{E}(G)$ 是 $\boldsymbol{S}(G)$ 的子半群。

设 σ, τ 是 G 的自同构，显然 $\sigma\tau$ 是自同态。又因一一变换的乘积还是一一变换，故 $\sigma\tau$ 是自同构。另外，恒等变换（$\boldsymbol{G}(G)$ 的单位元）是自同构，自同构 σ 的逆变换 σ^{-1} 也是自

同构．所以，$\boldsymbol{A}(G)$作成集合G的变换群（见§2·5和§3·6），或者说是$\boldsymbol{G}(G)$的子群．由于自同构是自同态和一一变换，故$\boldsymbol{A}(G)=\boldsymbol{E}(G)\cap\boldsymbol{G}(G)$．

证毕

例1 找出n阶循环群$G=\langle a\rangle$的自同态半群$\boldsymbol{E}(G)$和自同构群$\boldsymbol{A}(G)$．

解：$G=\{a, a^2,\cdots,a^n=e\}$．

（1）设σ是自同态，$\sigma(a)=a^k$，那末

$$\sigma(a^2)=\sigma(a)\sigma(a)=a^{2k},$$

$$\sigma(a^3)=\sigma(a)\sigma(a)\sigma(a)=a^{3k},$$

$$\cdots\cdots\cdots\cdots$$

$$\sigma(a^{n-1})=a^{(n-1)k},$$

$$\sigma(a^n)=a^{nk}=e.$$

因而σ形如：

$$\sigma(a^i)=a^{ki}\ (a^i\in G). \tag{1}$$

反之，（1）形的变换是G的自同态．这是因为对于$a^i,a^j\in G$，有

$$\sigma(a^ia^j)=\sigma(a^{i+j})=a^{k(i+j)}=a^{ki}\cdot a^{kj}=\sigma(a^i)\sigma(a^j).$$

所以，G共有n个自同态，分别对应（1）式中$k=1,2,\cdots,n$，当k是其他整数时，（1）式决定的同态与上面n个同态之一相等，即$|E(G)|=n=|G|$．

（2）设τ是自同构，那末τ也是自同态，应形如（1）式：$\sigma(a^i)=a^{ki}(a^i\in G)$．

假如k与n不互素，则最大公因数$l>1$，设$k=k_1l,n=n_1l$，那末$\tau(a^{n_1})=a^{kn_1}=a^{k_1ln_1}=a^{k_1n}=e$，$\tau(a^n)=a^{kn}=e$．而$a^{n_1}\neq a^n$，所以$\sigma$不是单射，因而$\sigma$不是自同构．

假如k与n互素，则

$$\sigma(a)=a^k,\ \sigma(a^2)=a^{2k},\cdots,\sigma(a^n)=a^{nk}=e$$

是两两不同的元素，因若$a^{ik}=a^{jk}$ ($1\leqslant i\leqslant j\leqslant n$)，则$e=a^{(j-i)k}$，说明$(j-i)k$是$n$的倍数，而$k$与$n$互素，只有$n\mid j-i, j=i$。所以$\sigma$是一一映射，因而是自同构。这就是说，$G$的自同构个数与小于$n$且与$n$互素的正整数个数相同。用$\varphi(n)$记小于$n$且与$n$互素的正整数个数，则$|A(G)|=\varphi(n)$。

注意：$\varphi(n)$称为欧拉(Euler)函数[注]，如$\varphi(2)=1$，$\varphi(3)=2$，$\varphi(4)=2$，$\varphi(5)=4$。

二、内自同构

设a是群G的元素。由a可以决定G的一个变换σ_a：

$$\sigma_a(x)=axa^{-1},\ (x\in G)。\tag{2}$$

定理 2 σ_a是群G的自同构。

证明：σ_a是满射。事实上，对于任意$g\in G$，方程$ax=ga$总有唯一解x。即有$b\in G$，使$aba^{-1}=g$或$\sigma_a(b)=g$。

σ_a是单射。事实上，如果$\sigma_a(x)=\sigma_a(y)$，则$axa^{-1}=aya^{-1}$。由群的消去律，$x=y$。

σ_a是自同态。事实上，当$x, y\in G$，有

$$\sigma_a(xy)=a(xy)a^{-1}=axa^{-1}aya^{-1}=\sigma_a(x)\sigma_a(y)。$$

总之，σ_a是G的自同构。

证毕

定义 1 上述自同构σ_a，称为由元素a决定的群G的内

注 L. Euler (1707—1783)瑞士人，历史上著名的数学家，他在数学的多方面均有重大贡献。晚年虽双目失明仍硕果垒垒。

自同构。群的其他自同构，称为**外自同构**。

对于可换群，$\sigma_a(x)=axa^{-1}=xaa^{-1}=x$。所以，这时内自同构只有恒等变换。就是说，可换群的任意自同构都是外自同构（除恒等变换外）。

例 2 在 3 次对称群 S_3 中，如果令

$$a=(1\quad 3\quad 2),$$

则 $a^{-1}=(2\quad 3\quad 1)=(1\quad 2\quad 3)$。这时，有

$$\sigma_a((1))=(1\quad 3\quad 2)(1)(1\quad 2\quad 3)=(1);$$

$$\sigma_a((1\quad 2))=(1\quad 3\quad 2)(1\quad 2)(1\quad 2\quad 3)=(1\quad 3);$$

$$\sigma_a((1\quad 3))=(1\quad 3\quad 2)(1\quad 3)(1\quad 2\quad 3)=(2\quad 3);$$

$$\sigma_a((2\quad 3))=(1\quad 3\quad 2)(2\quad 3)(1\quad 2\quad 3)=(1\quad 2);$$

$$\sigma_a((1\quad 2\quad 3))=(1\quad 3\quad 2)(1\quad 2\quad 3)(1\quad 2\quad 3)=(1\quad 2\quad 3);$$

$$\sigma_a((1\quad 3\quad 2))=(1\quad 3\quad 2)(1\quad 3\quad 2)(1\quad 2\quad 3)=(1\quad 3\quad 2).$$

内自同构在自同构群 $A(G)$ 中占有什么地位呢？

定理 3 群 G 的所有内自同构作成 $A(G)$ 的正规子群。

证明：设群 G 的所有内自同构构成集合

$$I(G)=\{\sigma_a \mid a\in G\}.$$

$I(G)$ 作成 $A(G)$ 的子群。

事实上，任取 σ_a，$\sigma_b\in I(G)$，则对于 $x\in G$，有

$$\begin{aligned}\sigma_a\sigma_b(x)&=\sigma_a(\sigma_b(x))=\sigma_a(bxb^{-1})\\&=\sigma_a(b)\cdot\sigma_a(x)\cdot\sigma_a(b^{-1})=aba^{-1}axa^{-1}ab^{-1}a^{-1}\\&=abxb^{-1}a^{-1}=(ab)x(ab)^{-1}=\sigma_{ab}(x).\end{aligned}$$

即 $\sigma_a\sigma_b=\sigma_{ab}\in I(G)$。

恒等变换 $\varepsilon_G=\sigma_e\in I(G)$。

σ_a 既然是同构，其逆σ_a^{-1} 也是G的自同构（见§2·5）。对于 $x\in G$， 设 $\sigma_a^{-1}(x)=y$， 则 $\sigma_a(y)=x$， $aya^{-1}=x$， $y=a^{-1}xa=a^{-1}x(a^{-1})^{-1}=\sigma_{a^{-1}}(x)$， $\sigma_a^{-1}=\sigma_{a^{-1}}\in \boldsymbol{I}(G)$。

根据§3·3 定理 1，$\boldsymbol{I}(G)$是$\boldsymbol{A}(G)$的子群。

$\boldsymbol{I}(G)$作成$\boldsymbol{A}(G)$的正规子群。

事实上，设 φ 是群G的任意自同构，$\sigma_a\in \boldsymbol{I}(G)$，则对于$x\in G$，有

$$
\begin{aligned}
(\varphi\sigma_a\varphi^{-1})(x) &= \varphi(\sigma_a(\varphi^{-1}(x))) = \varphi(a\varphi^{-1}(x)a^{-1}) \\
&= \varphi(a)\varphi(\varphi^{-1}(x))\varphi(a^{-1}) = \varphi(a)x\varphi(a)^{-1} \\
&= \sigma_{\varphi(a)}(x).
\end{aligned}
$$

即 $\varphi\sigma_a\varphi^{-1}=\sigma_{\varphi(a)}\in \boldsymbol{I}(G)$。

根据§3·8 定理 3，$\boldsymbol{I}(G)$是$\boldsymbol{A}(G)$的正规子群。

证毕

群的每个元素都可以决定一个内自同构，但不同的元素可以决定相同的内自同构。如可换群任何元素决定的内自同构都是恒等自同构。对于非可换群G，G和$\boldsymbol{I}(G)$也不一定能有一一对应。下面的定理，揭示了G、$\boldsymbol{I}(G)$及群中心C之间的关系。

定理 4 群G的内自同构群与G关于中心的商群同构，即$\boldsymbol{I}(G)\cong G/C$。

注意：群G的中心是正规子群，故G/C有意义。

证明：建立G到$\boldsymbol{I}(G)$的映射 φ 为：

$$\varphi(a)=\sigma_a,\ (a\in G).$$

显然 φ 是满射。φ 还是同态。事实上，由定理 3 的证明，

$$\varphi(ab)=\sigma_{ab}=\sigma_a\sigma_b=\varphi(a)\varphi(b).$$

φ 的同态核 K_φ 是满足 $\sigma_a=\varepsilon_G$（恒等变换） 的元素 a 的集合，

即对于任意 $x\in G$，适合 $axa^{-1}=x$ 的元素 a 的集合．上式等价于 $ax=xa$，所以 a 与 G 的每个元素可换，即 $a\in C$（G的中心）．总之，$K_\varphi=C$．根据同态基本定理，

$$G/C\cong \boldsymbol{I}(G).$$

证毕

定理 4 说明，一般说来，内自同构要比G的元素来得"少"．因为两个元素如果相差一个属于中心的元素，说明它们在C的同一陪集里，因而产生同一内自同构．

例 3　正方形对称群 D_4 的中心是$\{R_{2\pi}, R_\pi\}$（见§3·8例2），因而其内自同构有$\frac{8}{2}=4$个．

习　题　3·11

1．下列变换哪些是$\langle C^*, \cdot\rangle$的自同态？哪些是自同构？

(1) $\sigma_1(z)=\bar{z}$；

(2) $\sigma_2(r(\cos\varphi+i\sin\varphi))=r^2(\cos\varphi+i\sin\varphi)$；

(3) $\sigma_3(r(\cos\varphi+i\sin\varphi))=r\left[\cos\left(\varphi+\frac{\pi}{2}\right)+i\sin\left(\varphi+\frac{\pi}{2}\right)\right]$；

(4) $\sigma_4(r(\cos\varphi+i\sin\varphi))=r$．

2．设φ是群G的自同构．求证：对于任意的$a\in G$，a与$\varphi(a)$同阶．

3．找出无限循环群的自同态半群与自同构群．

4．求证：群G的变换$\sigma(a)=a^{-1}(a\in G)$是自同构的充要条件为G是可换群．

5．写出克莱茵四元群 B_4 的自同构群．求证：$\mathbf{A}(B_4)\cong$

S_3.

6. 群G的子群H是正规子群的充要条件是G的任意内自同构都使H不变。试证明之。

7. 设群G的自同构只有恒等变换，求证：G是可换群，且每个元素满足$x^2=e$。

*8. 设φ是群G的自同构，求证：$a\to\varphi(a)a^{-1}$是单射的充要条件为φ的不动元只有e。

§3·12 群的直积

由已知群可以产生出新的群来，商群就是一例，另外常见的是群的直积。群的直积分解，也是剖析群结构的重要方法。本节除介绍直积概念外，还介绍可换群分解为循环群直积的方法，即有限生成可换群基本定理。

一、直积的概念

设$\langle G,\cdot\rangle$和$\langle H,\cdot\rangle$是两个群（为简便计，其乘法用同一符号表示）。积集$G\times H$由一切形如(g,h)的元素组成，其中$g\in G$，$h\in H$。在$G\times H$中引入法则：

$$(g_1,h_1)\cdot(g_2,h_2)=(g_1g_2,h_1h_2)。\tag{1}$$

显然(1)所示的法则是$G\times H$的代数运算，称为$G\times H$的乘法。

$\langle G\times H,\cdot\rangle$是群。事实上，结合律由原来两个群的乘法结合律保证；单位元显然是(e_G,e_H)，其中e_G和e_H分别是群G和群H的单位元；(g,h)的逆元是(g^{-1},h^{-1})。

定义1 群$\langle G\times H,\cdot\rangle$称为群$\langle G,\cdot\rangle$和群$\langle H,\cdot\rangle$的直积。

$\langle G\times H,\cdot\rangle$也可记作$G\times H$。

如果G，H是有限群，显然$|G\times H|=|G|\cdot|H|$。

多个群的直积也可以类似地定义。n个群$\langle G_i,\cdot\rangle, i=1,2,\cdots,n$的直积，记为

$$\langle G_1\times G_2\times\cdots\times G_n,\cdot\rangle,$$

或直接记为$G_1\times G_2\times\cdots\times G_n$。其运算规定为

$$\begin{aligned}&(g_1,g_2,\cdots,g_n)\cdot(h_1,h_2,\cdots,h_n)\\&=(g_1h_1,g_2h_2,\cdots,g_nh_n)\end{aligned} \tag{2}$$

单位元是$(e_1,e_2,\cdots,e_n)$，其中$e_1,e_2,\cdots,e_n$分别是$G_1,G_2,\cdots,G_n$的单位元。$(g_1,g_2,\cdots,g_n)$的逆元是$(g_1^{-1},g_2^{-1},\cdots,g_n^{-1})$。

例1 写出$C_1\times C_2$的乘法表。

注意：C_2表二阶循环群(见§3·5)。

证明：设$C_2=\{e,a\}, a^2=e$。

$$C_2\times C_2=\{(e,e),(e,a),(a,e),(a,a)\}.$$

根据群直积的定义，有以下乘法表：

$\cdot$	(e,e)	(e,a)	(a,e)	(a,a)
(e,e)	(e,e)	(e,a)	(a,e)	(a,a)
(e,a)	(e,a)	(e,e)	(a,a)	(a,e)
(a,e)	(a,e)	(a,a)	(e,e)	(e,a)
(a,a)	(a,a)	(a,e)	(e,a)	(e,e)

与§3·1例4中B_4的乘法对照，可见$C_2\times C_2\cong B_4$。

例2 求证：任意4阶群或者是C_4，或者同构于B_4。

证明：设G是4阶群。如果G中有4阶元，设为a，那末a,a^2,a^3,a^4是G中不同的元素。所以a是G的生成元，G是4阶循环群。

如果G中没有四阶元，设$G=\{a,b,c,e\}$.由拉格朗日定理的推论(§3·4 定理 4),所有元素的阶是 4 的因子，因而只能是 2 或 1 . 这时非单位元的阶都是 2 ，即 $a^2=b^2=c^2=e$. 而 ab 不能等于 a 或 b ，否则由消去律，得 $b=e$ 或 $a=e$.ab 也不能等于 e ，否则由 $ab=e=a^2$，推得 $a=b$. 因而只有 $ab=c$. 同理 $ba=c$，$ac=ca=b$，$bc=cb=a$，与例 1 比较，如建立映射：$e\to(e,e)$，$a\to(e,a)$，$b\to(a,e)$，$c\to(a,a)$，刚好是同构映射，即 $G\cong C_2\times C_2\cong B_4$.

二、可分解群与不可分解群

定义 2 一个群如果同构于其真子群的直积，则称为可分解群，否则称为不可分解群.

从例 2 可见， 4 阶非循环群 $B_4=\{a,b,c,e\}$ 是可分解的，因为它同构于两个 2 阶循环子群的直积：$G\cong\{e,a\}\times\{e,b\}$.

例 3 求证：$\langle \mathbf{R}^*,\cdot\rangle$是可分解群.

分析： 证明$\langle \mathbf{R}^*,\cdot\rangle\cong\langle\{1,-1\},\cdot\rangle\times\langle \mathbf{R}^+,\cdot\rangle$.

证明： 构造 $\mathbf{R}^*$ 到 $\{1,-1\}\times \mathbf{R}^+$ 的映射 σ：

$$\sigma(x)=\begin{cases}(1,x),\text{当 } x>0;\\(-1,-x),\text{当 } x<0.\end{cases}$$

σ 显然是一一映射，下面证其是同构.

任取 $x_1,x_2\in \mathbf{R}^*$,

(1) 如果 $x_1>0$，$x_2>0$，则

$$\begin{aligned}\sigma(x_1x_2)&=(1,x_1x_2)\\&=(1,x_1)(1,x_2)\\&=\sigma(x_1)\sigma(x_2);\end{aligned}$$

(2) 如果 $x_1<0$，$x_2<0$，则

$$\sigma(x_1x_2)=(1,x_1x_2)$$
$$=(-1,-x_1)(-1,-x_2)$$
$$=\sigma(x_1)\sigma(x_2);$$

(3) 如果 $x_1>0$，$x_2<0$，则

$$\sigma(x_1x_2)=(-1,-x_1x_2)$$
$$=(1,x_1)(-1,-x_2)$$
$$=\sigma(x_1)\sigma(x_2).$$

因而，σ 是同构映射，即

$$\langle \boldsymbol{R}^*,\cdot\rangle\cong\langle\{1,-1\},\cdot\rangle\times\langle \boldsymbol{R}^+,\cdot\rangle.$$

右端两个直积因子都是$\langle \boldsymbol{R}^*,\cdot\rangle$的真子群，所以，$\langle \boldsymbol{R}^*,\cdot\rangle$是可分解群。

判断一般的群是否可分解，并不简单，但对循环群来说，却非常容易，只看它的阶就可以。下面讨论这个问题：

定理1 如果m与n互素，则 C_{mn} 同构于 $C_m\times C_n$。

证明：设 $C_{mn}=\langle a\rangle,C_m=\langle b\rangle,C_n=\langle c\rangle$，其单位元是 e，e_1,e_2。规定$\langle a\rangle$到$\langle b\rangle\times\langle c\rangle$的对应法则为：

$$\sigma(a^r)=(b^r,c^r).$$

σ 是映射。事实上，如果 $a^{r_1}=a^{r_2}$，则 $mn|r_1-r_2$，因而 $m|r_1-r_2$，$n|r_1-r_2$，所以 $b^{r_1}=b^{r_2}$，$c^{r_1}=c^{r_2}$，$(b^{r_1},c^{r_1})=(b^{r_2},c^{r_2})$。

σ 是同态。事实上，我们有

$$\sigma(a^{r_1}a^{r_2})=\sigma(a^{r_1+r_2})$$
$$=(b^{r_1+r_2},c^{r_1+r_2})$$
$$=(b^{r_1}b^{r_2},c^{r_1}c^{r_2})$$
$$=(b^{r_1},c^{r_1})(b^{r_2},c^{r_2})$$

$$=\sigma(a^{r_1})\sigma(a^{r_2}).$$

σ 是同构．事实上，设 K_σ 是 σ 的同态核，$a^r\in K_\sigma$，则

$$(e_1,e_2)=\sigma(a^r)=(b^r,c^r),$$

即 $b^r=e_1$，$c^r=e_2$，r 是 m，n 的公倍数．又因 $(m,n)=1$，故 $mn|r$，$a^r=e$．所以 $K_\sigma=\{e\}$，$\langle a\rangle$ 与象集 $\sigma[\langle a\rangle]$ 同构．

$\sigma[\langle a\rangle]$ 的阶等于 $\langle a\rangle$ 的阶，即 mn，因而 σ 是满射．总之，$\langle a\rangle\cong\langle b\rangle\times\langle c\rangle$．

证毕

$\langle a\rangle=C_{mn}$ 的元素 a^n 生成的子群 $\langle a^n\rangle$ 是 m 阶循环群，a^m 生成的子群 $\langle a^m\rangle$ 是 n 阶循环群，它们都是 $\langle a\rangle$ 的真子群．C_{mn} 同构于两个真子群的直积，所以 C_{mn} 是可分解群．

如 $C_{20}\cong C_5\times C_4$，$C_{30}\cong C_3\times C_{10}\cong C_6\times C_5\cong C_{15}\times C_2$．

定理 1 还可进一步引伸：

定理 2 设 $n=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$，其中 $p_1,p_2,\cdots,p_r$ 是不同的素因子，则

$$C_n\cong C_{p_1^{t_1}}\times C_{p_2^{t_2}}\times\cdots\times C_{p_r^{t_r}}.$$

证明：设 $m=p_2^{t_2}\cdots p_r^{t_r}$，显然 m 与 $p_1^{t_1}$ 互素，由定理 1，

$$C_n\cong C_{p_1^{t_1}}\times C_m.$$

继续使用定理 1，得到 $C_n\cong C_{p_1^{t_1}}\times C_{p_2^{t_2}}\times\cdots\times C_{p_r^{t_r}}$．

证毕

如 $100=2^2\cdot5^2$，$300=3\cdot2^2\cdot5^2$，故

$$C_{100}\cong C_4\times C_{25},$$
$$C_{300}\cong C_3\times C_4\times C_{25}.$$

根据定理 2，我们可以将有限循环群化为素数幂阶循环群的直积．那末，素数幂阶的循环群是不是可分解的呢？

定理 3 素数幂阶的循环群是不可分解群．

证明：素数幂 p^n 的真因子只有 p，p^2，…，p^{n-1}，因而 C_{p^n}的真子群的阶只能是 p，p^2，…，p^{n-1}。如果 $C_{p^n} \cong C_{p^t} \times C_{p^r}$，则 $C_{p^t} \times C_{p^r}$ 是 p^n 阶循环群。设其生成元为(b,c)，其中 $b \in C_{p^t}$，$c \in C_{p^r}$。不妨设 $t \geq r$，这时，

$$(b,c)^{p^t} = (b^{p^t}, c^{p^t}) = (e_1, e_2),$$

其中 e_1 和 e_2 分别是 C_{p^t} 和 C_{p^r} 的单位元。(b,c)的阶不大于 p^t，而 $p^t < p^n$，出现矛盾。所以，C_{p^n} 不可分解。

证毕

此外还有

定理 4 C_∞ 不可分解。

证明：$C_\infty = \langle a \rangle$的任意子群也是形如$\langle a^n \rangle$的循环群。假如$\langle a \rangle$可分解，设

$$\langle a \rangle \cong \langle a^m \rangle \times \langle a^n \rangle,$$

则 $m \neq 0$，$n \neq 0$（否则，$\langle a^m \rangle$和$\langle a^n \rangle$是$\langle a \rangle$的平凡子群）。再设 a 的同构象是(a^{km}, a^{hn})，对于$\langle a \rangle$的任意元素 a^s，其同构象应为(a^{skm}, a^{shn})。k 和 h 不等于零，否则 $\langle a \rangle$ 的同构象集不是 $\langle a^m \rangle \times \langle a^n \rangle$。取

$$(a^{2km}, a^{hn}) \in \langle a^m \rangle \times \langle a^n \rangle.$$

设其逆象为 $a^t \in \langle a \rangle$，而 a^t 的象为

$$(a^{tkm}, a^{thn}) \neq (a^{2km}, a^{hn}).$$

推出矛盾。

证毕

综合以上几个定理，得到判断任意循环群是否可分解的准则：

定理 5 循环群可分解的充要条件是：

（1）阶数有限；

（2）阶数不是素数幂，也不是1，即阶数至少有两个不同的素因子。

另外，由于任何正整数都有素因子分解式，故有

定理6 任意有限循环群总同构于若干素数幂阶循环子群的直积。

三、可换群基本定理

循环群毕竟过于简单，它的生成系只含一个元素，复杂一些的要算有限生成的可换群，即由有限集生成的可换群。例如有限可换群及循环群都是有限生成的可换群，而有理数加群就不是这样的群。以下的工作，是设法剖析有限生成的可换群的结构，使其表为不可分解循环群的直积。循环群是最简单的群，这样对群进行讨论或分类无疑是很有利的。

定理7（可换群基本定理） 有限生成的可换群同构于有限个不可分解循环子群的直积。

为证明这个定理，引进

定义3 设G是群，$\{a_1,a_2,\cdots,a_s\}$是其一个生成系，且G的任意一个生成系所含元素个数不少于s，则称$\{a_1, a_2, \cdots, a_s\}$是$G$的最小生成系。

显然，有限生成的可换群总有最小生成系。

引理1 设$\{x_1,x_2,\cdots,x_s\}$是可换群G的一个生成系，$k_1, k_2,\cdots,k_s$是整体互素的整数（即$(k_1, k_2, \cdots, k_s)=1$），$y=x_1^{k_1}x_2^{k_2}\cdots x_s^{k_s}$，则存在$s-1$个元素，使其与$y$作成$G$的生成系。

证明：对s施行归纳法。

当$s=1$时，引理显然正确。

当$s=2$时，由k_1与k_2互素，知存在整数c_1，c_2，使

$c_1k_1+c_2k_2=1$。从而

$$x_1=(x_1^{k_1}x_2^{k_2})^{c_1}(x_1^{c_2}x_2^{-c_1})^{k_2},$$

$$x_2=(x_1^{k_1}x_2^{k_2})^{c_2}(x_1^{c_2}x_2^{-c_1})^{-k_1}.$$

这时，$G=\langle x_1,x_2\rangle=\langle y,x_1^{c_2}x_2^{-c_1}\rangle$。

现在假定引理对 $s-1$ 成立，推证定理对 s 成立。

设 $k_i=l_id, i=1,\cdots,s-1$，$d=(k_1,\cdots,k_{s-1})$，因而 $(l_1,\cdots,l_{s-1})=1$。设 $y_1=x_1^{l_1}\cdots x_{s-1}^{l_{s-1}}$. 由归纳假定，存在 $y_2,\cdots,y_{s-1}$，使

$$\langle x_1,\cdots,x_{s-1}\rangle=\langle y_1,\cdots,y_{s-1}\rangle.$$

因而，$G=\langle y_1,\cdots,y_{s-1},x_s\rangle$。

但是，$y=y_1^dx_s^{k_s}$，且 d 与 k_s 互素。由 $s=2$ 的情况的证明，存在 z，使 $\langle y,z\rangle=\langle y_1,x_s\rangle$。所以

$$G=\langle y_1,\cdots,y_{s-1},x_s\rangle=\langle y,y_2,\cdots,y_{s-1},z\rangle.$$

证毕

以下是定理 7 的

证明：设 G 的最小生成系含 s 个元素。下面证明 G 同构于 s 个循环子群的直积。

当 $s=1$ 时，G 是循环群，定理显然正确。

设当 $s-1$ 时定理正确，推证定理对 s 成立。事实上，设 $\{x_1,\cdots,x_s\}$ 是 G 的这样一个最小生成系，其中 x_s 是各个最小生成系中阶最小的，设其阶为 m。假定 $H=\langle x_1,\cdots,x_{s-1}\rangle$，则 H 是 G 的真子群。按归纳假定，H 同构于 $s-1$ 个循环子群的直积。

$H\cap\langle x_s\rangle=\{e\}$。事实上，如果不然，存在整数 $k_s<m$ 和整数 $k_1,\cdots,k_{s-1}$，使 $x_1^{k_1}\cdots x_{s-1}^{k_{s-1}}=x_s^{k_s}$，即 $x_1^{k_1}\cdots x_{s-1}^{k_{s-1}}x_s^{-k_s}=e$。设 $d=(k_1,\cdots,k_{s-1},k_s)$，则

$$(k_1d^{-1},\cdots,k_{s-1}d^{-1},\ -k_sd^{-1})=1.$$

由引理 1，元素 $x_1^{k_1d^{-1}}\cdots x_{s-1}^{k_{s-1}d^{-1}}x_s^{-k_sd^{-1}}$ 是某最小生成系的一个元素，其阶 $\leqslant d$。然而 $d\leqslant k_s<m$，与 m 的选取矛盾。

构造 $H\times\langle x_s\rangle$ 到 G 的映射 φ 如下：

$$\varphi((h,x_s^k))=hx_s^k.$$

显然，φ 是同态。其核为

$$\begin{aligned}K_\varphi&=\{(h,x_s^k)\mid hx_s^k=e,h\in H,k\in\mathbf{Z}\}\\&=\{(h,x_s^k)\mid h=x_s^{-k},h\in H,k\in\mathbf{Z}\}\\&=\{(e,e)\}.\ (\text{由于 } H\cap\langle x_s\rangle=\{e\})\end{aligned}$$

因而 φ 为单同态。又因 $G=\langle H,x_s\rangle$，所以 φ 是满射。总之，φ 是同构，$H\times\langle x_s\rangle\cong G$。

由归纳假定，H 同构于 $s-1$ 个循环子群的直积，因而 G 同构于 s 个循环子群的直积。由定理 6，每个有限循环子群又同构于若干素数幂阶循环子群的直积。所以 G 同构于有限个素数幂阶循环子群及无限循环子群的直积，即有限个不可分解循环群的直积。

证毕

推论 1 有限可换群同构于有限个素数幂阶循环子群的直积：

$$G\cong C_{p_1^{t_1}}\times C_{p_2^{t_2}}\times\cdots\times C_{p_r^{t_r}},\tag{3}$$

其中 $p_1,p_2,\cdots,p_r$ 是素数（可以相同），且 $|G|=p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$。

可以证明，同一个有限生成的可换群在上述意义下展成不可分解循环子群的直积时，各种不同的分解方式彼此同构。同时，对于 n 阶可换群而言，n 的不同素数方幂的分解方法（不计因子次序）对应的循环群的直积是互不同构的，因而 n 有几种不同素数方幂的分解方法，n 阶可换群就有几个同

构类。

如 $100=2^2\cdot5^2=2\cdot2\cdot5^2=2^2\cdot5\cdot5=2\cdot2\cdot5\cdot5$，所以 100 阶可换群共有 4 种互不同构的结构：

$$C_4\times C_{25},\quad C_2\times C_2\times C_{25},$$
$$C_4\times C_5\times C_5, C_2\times C_2\times C_5\times C_5.$$注

$8=2^3=2^2\cdot2=2\cdot2\cdot2$，所以 8 阶可换群共有 3 种互不同构的结构：

$$C_8,\quad C_4\times C_2,\quad C_2\times C_2\times C_2.$$

所有的 n 阶可换群分成互不同构的类，每类都同构于(3)形的循环群直积，叫做 n 阶可换群的同构分类。如 100 阶可换群共有 4 个同构类，8 阶可换群共有 3 个同构类。

必须指出，n 的上述分解，每个因子必须是素数方幂，如 100 不能分解成 $50\cdot2$ 或 $20\cdot5$ 等。当 $n=pq$(p, q 为不同的素数)时，n 阶可换群群同构于 $C_p\times C_q\cong C_{pq}$，即是循环群。如 10 阶、6 阶、15 阶、35 阶可换群都是循环群。

由有限可换群基本定理，我们可以得出一个有趣的结果，它是拉格朗日定理对于可换群的逆命题。

定理 8 如 m 是 n 的因子，则 n 阶可换群 G 中，必有 m 阶子群。

证明：假定 $G\cong C_{p_1^{t_1}}\times\cdots\times C_{p_r^{t_r}}$，其中 $n=p_1^{t_1}\cdots p_r^{t_r}$. 由于 $m|n$，故 m 可写成 $m=p_1^{l_1}\cdots p_r^{l_r}$，其中 $l_i\leqslant t_i$，$i=1,\cdots,r$。$p_i^{l_i}|p_i^{t_i}$，所以 $C_{p_i^{t_i}}$ 必有 $p_i^{l_i}$ 阶循环子群 $C_{p_i^{l_i}}$。令

$$\bar{H}=C_{p_1^{l_1}}\times\cdots\times C_{p_r^{l_r}},$$

注 它们互不同构是显然的，如第一个群有 25 阶元和 4 阶元，第二个群只有 25 阶元无 4 阶元，第三个群只有 4 阶元无 25 阶元，第四个群两种元素都没有。

显然 $\bar{H}$ 是 $\bar{G}=C_{p_1^{l_1}}\times\cdots\times C_{p_r^{l_r}}$ 的子群，$\bar{H}$ 的阶为 $p_1^{l_1}\cdots p_r^{l_r}=m$。

由于 $G\cong\bar{G}$，$\bar{H}$ 在 G 中对应的子群 H 就是 G 的 m 阶子群。

证毕

习 题 3·12

1. 设 $G=G_1\times G_2$，$\bar{G}_1=\{(g_1,e_2)\mid g_1\in G_1\}$，$\bar{G}_2=\{(e_1,g_2)\mid g_2\in G_2\}$，求证：$\bar{G}_1$，$\bar{G}_2$ 是 G 的正规子群且 $G_1\cong\bar{G}_1$，$G_2\cong\bar{G}_2$，$G/\bar{G}_1\cong G_2$，$G/\bar{G}_2\cong G_1$。

2. 求证：群的直积的中心等于各因子中心的直积。

3. 设 G_1，G_2 是群，求证：$G_1\times G_2\cong G_2\times G_1$。

4. C_{60} 是否同构于 $C_{10}\times C_6$？

5. D_4 是否同构于 $C_4\times C_2$？

6. 分析 625 阶可换群的同构分类。

7. 分析 120 阶可换群的同构分类。

8. 下列群是否可分解？

(1) C_{625}；(2) C_{49}；(3) C_{111}；(4) C_{527}。

9. 求证：$\{(1\ \ 2),(1\ \ 2\ \ 3)\}$ 是 S_3 的最小生成系。

§3·13 西洛定理

有限群是一类重要的群，本节讨论它的结构，介绍著名的西洛定理。为此先讲几个预备知识。

一、共轭类

定义 1 设 x，y 是群 G 的元素，如果存在 $a\in G$，使

$axa^{-1}=y$，则称 x 与 y 共轭，y 是 x 的共轭元.

就是说，x 与 y 共轭当且仅当存在一个内自同构，把 x 变为 y.

共轭显然是关系，它也是等价关系，因为

对于任意的 $x\in G$，$x=exe^{-1}$，故 x 与自身共轭；

如果 x 与 y 共轭，即有 $a\in G$，使 $axa^{-1}=y$，则 $y=a^{-1}xa=a^{-1}x(a^{-1})^{-1}$，即 y 与 x 共轭；

如果 x 与 y 共轭，y 与 z 共轭，则有 a，$b\in G$，$axa^{-1}=y$，$byb^{-1}=z$，因而

$$z=b(axa^{-1})b^{-1}=(ba)x(ba)^{-1},$$

即 x 与 z 共轭.

等价关系决定一种分类，这样，在群 G 中就可以划分为若干共轭类，两个元素同类当且仅当它们共轭. 显然，一个共轭类是其中任一元素在所有内自同构下象的集合.

例 1　写出 S_3 的共轭类.

解：(1) 只与自己共轭，因为单位元在自同构下不变.

$(1\ \ 2)$，$(1\ \ 3)$，$(2\ \ 3)$同类，这是因为

$$(2\ \ 3)(1\ \ 3)(2\ \ 3)^{-1}=(1\ \ 2),$$

$$(1\ \ 2)(2\ \ 3)(1\ \ 2)^{-1}=(1\ \ 3).$$

$(1\ \ 2\ \ 3)$与$(1\ \ 3\ \ 2)$同类，这是因为

$$(1\ \ 2)(1\ \ 2\ \ 3)(1\ \ 2)^{-1}=(1\ \ 3\ \ 2).$$

而(1)，$(1\ \ 2)$，$(1\ \ 2\ \ 3)$互不同类，所以 S_3 的共轭类共三个：

$$\{(1)\},\ \{(1\ \ 2),\ (1\ \ 3),(2\ \ 3)\},$$

$$\{(1\ \ 2\ \ 3),(1\ \ 3\ \ 2)\}.$$

由此可见，群的共轭类含的元素不一定个数相同. 例如

含单位元 e 的共轭类，就只有一个元素，因为 $aea^{-1}=e$ 对所有元素 $a\in G$ 成立。不仅如此，群中心的每个元素也有这个性质。

定理 1 群的一个共轭类当且仅当包含中心的元素时，是单元素集。

证明：设 $\{a\}$ 是一个共轭类，则对任意 $x\in G$，$xax^{-1}=a$，或 $xa=ax$，即 a 与 G 中所有元素可换，a 属于中心 C。

反之，设一个共轭类中含有 $a\in C$，则 a 与 G 的任意元素 x 可换，$xa=ax$，$xax^{-1}=a$，a 是内自同构下的不变元，因而这个共轭类是单元素集 $\{a\}$。

证毕

例 2 写出正方形对称群 D_4 的共轭类。

解：D_4 的中心是 $\{R_{2\pi}, R_\pi\}$，故 $\{R_{2\pi}\}$，$\{R_\pi\}$ 是两个共轭类。

$R_{\frac{\pi}{2}}$ 的共轭元有

$$R_{\frac{\pi}{2}}R_{\frac{\pi}{2}}R_{\frac{\pi}{2}}^{-1}=R_\pi R_{\frac{\pi}{2}}R_\pi^{-1}=R_{\frac{3}{2}\pi}R_{\frac{\pi}{2}}R_{\frac{3}{2}\pi}^{-1}$$
$$=R_{2\pi}R_{\frac{\pi}{2}}R_{2\pi}^{-1}=R_{\frac{\pi}{2}};$$

$HR_{\frac{\pi}{2}}H^{-1}=VR_{\frac{\pi}{2}}V^{-1}=D_1R_{\frac{\pi}{2}}D_1^{-1}=D_2R_{\frac{\pi}{2}}D_2^{-1}=R_{\frac{3}{2}\pi}$. 所以，$\{R_{\frac{\pi}{2}}, R_{\frac{3}{2}\pi}\}$ 是一个共轭类。

同样可知其他两个共轭类：

$$\{H,V\},\ \{D_1,D_2\}.$$

群 D_4 有 8 个元素，每个元素对应一个内自同构，这 8 个内自同构作用 $R_{\frac{\pi}{2}}$，却只有两个不同的象。这是什么原因呢？

定理2 有限群 G 中元素 a 共轭元的个数等于正规化子 $N(a)$ 在 G 中的指数，因而是 $|G|$ 的因子。

注意：正规化子概念见§3·3。

证明：任取 $N(a)$ 的一个左陪集 $gN(a)$ 中的元素 gn，则

$$(gn)a(gn)^{-1}=gnan^{-1}g^{-1}=gann^{-1}g^{-1}=gag^{-1}.$$

所以，$N(a)$ 的同一左陪集的元素生成 a 的同一共轭元。

反之，设 $g_1ag_1^{-1}=gag^{-1}$，则 $(g^{-1}g_1)a=a(g^{-1}g_1)$。即 $g^{-1}g_1\in N(a)$，g 与 g_1 在 $N(a)$ 的同一左陪集中。

总之，$N(a)$ 的所有左陪集的集合与 a 所在的共轭类有一一对应，即 a 的共轭元个数等于 $N(a)$ 的左陪集数，即等于 $N(a)$ 在 G 中的指数。

证毕

在例1中，$N((1\ \ 2))=\{(1\ \ 2),\ (1)\}$，其指数为3，故 $(1\ \ 2)$ 有3个共轭元。而

$$N((1\ \ 2\ \ 3))=\{(1\ \ 2\ \ 3),(1\ \ 3\ \ 2),(1)\}$$

的指数为2，故 $(1\ \ 2\ \ 3)$ 有两个共轭元。

例2中，$a=R_{\frac{\pi}{2}}$ 的正规化子

$$N(a)=\{R_{\frac{\pi}{2}},\ R_{\pi},\ R_{\frac{3}{2}\pi},\ R_{2\pi}\}$$

的指数为2，故 a 有两个共轭元。

二、群方程

在有限群 G 中，其所有共轭类的并是 G。群中心的每个元素独成一类，设其他各类为 P_1，P_2，…，P_r，则 $|P_i|>1$，$i=1$，2，…，r，

$$|G|=|C|+|P_1|+|P_2|+\cdots+|P_r|. \tag{1}$$

等式(1)称为群方程。

注意：(1)的各项都是正整数，不是集合。

如：S_3 的群方程是 $6=1+2+3$，D_4 的群方程是 $8=2+2+2+2$，n 阶可换群的中心与整个群重合，其群方程最简单：$n=n$。

定义 2 如果一个群的阶是素数 p 的方幂，则称之为有限 p 群，或 p 群。注

如 2 阶群、3 阶群、4 阶群、8 阶群都是 p 群。1 阶群也是 p 群，称为平凡 p 群。

定理 3 非平凡 p 群的中心也是非平凡 p 群。

证明：设群 G 的阶为 p^n $(n>0)$，在等式(1)中，p 整除 $|G|$。由定理 2，$|P_i|$ 是 $|G|$ 的真因子，p 是素数，故 p 整除各个 $|P_i|$。因而 p 整除 $|C|$。C 是 G 的子群，由拉格朗日定理，$|C|$ 是 p 的正整数方幂，即 C 是非平凡 p 群。

证毕

三、西洛(Sylow)定理注

按照拉格朗日定理，有限群子群的阶是群阶的因子。这个定理的逆命题对可换群是成立的(见上节)，但对于非可换群并不成立。就是说，如果 m 整除 n，n 阶群中不一定有 m 阶子群。如 4 次交错群 A_4 是 12 阶群：

$$A_4=\{(1),\ (1\ 2\ 3),(1\ 2\ 4),(1\ 3\ 2),(1\ 3\ 4),\\ (1\ 4\ 2),(1\ 4\ 3),(2\ 3\ 4),(2\ 4\ 3),$$

注　有的书将 p 群规定为所有元素的阶都是固定素数 p 的方幂的群，即可以是无限群，与这里定义不同。

注　L. Sylow(1832—1918)，挪威数学家。

$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

它有1阶、2阶、3阶、4阶子群，却没有6阶子群.

下面从另一角度来寻觅类似拉格朗日逆命题的定理，这就是著名的西洛定理.

定理 4 设 p 是素数. 如果 $p^k(k\geqslant 1)$ 整除群 G 的阶，则 G 包含 p^k 阶子群.注

证明：对群 G 的阶数实行数学归纳法.

如果 $|G|=1$，定理显然成立.

假定定理对于阶数小于 n 的群成立，下面证明定理对阶数等于 n 的群 G 成立.

写出群 G 的群方程

$$|G|=|C|+|P_1|+\cdots+|P_r|.$$

(r 可以等于零，这时 G 是可换群)

分两种情况讨论：

(1) 如果 $p\nmid|C|$. 由于 $p\,\big|\,|G|$，则至少有一个共轭类 P_i，使 $p\nmid|P_i|$. 取 P_i 中的一个元素 y，y 的正规化子 $N(y)$ 的阶 $|N(y)|$ 与 $|P_i|$ 之积等于 $|G|$ (定理2). p 是素数，$p\nmid|P_i|$，故 $p^k\,\big|\,|N(y)|$，说明 $N(y)$ 不是单元素集，$|N(y)|<|G|$. 由归纳假定，群 $N(y)$ 有一个 p^k 阶子群，它自然也是群 G 的子群.

(2) 如果 $p\,\big|\,|C|$，由上节定理8，可换群 C 包含一个 p 阶子群 C_1，C_1 是 G 的中心 C 的子群，必是 G 的正规子群，这是因为对任意的 $g\in G$，$c\in C_1$，有

$$gcg^{-1}=cgg^{-1}=c.$$

注 西洛定理还包括其他一些内容，这里从略.

群G/C_1的阶$\frac{|G|}{p}<n$. 由于$p^k \mid |G|$，故$\frac{|G|}{p}$是p^{k-1}的倍数。按归纳假定，G/C_1应包含一个p^{k-1}阶子群，由于G与G/C_1同态，根据子群间的对应关系（§3·10推论1），这个p^{k-1}阶子群形如H/C_1，其中H是G的子群．这时，

$$|H/C_1| = \frac{|H|}{|C_1|}.$$

$$|H| = |H/C_1| \cdot |C_1| = p^{k-1} \cdot p = p^k$$

于是，找到一个p^k阶子群$H \subseteq G$.

证毕

任何一个有限群G的阶m，是一个正整数，它可以唯一地分解为不同素数方幂之积：

$$m = p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}.$$

西洛定理断言，G一定有p_1阶，p_1^2阶，…，$p_1^{i_1}$阶，p_2阶，p_2^2阶，…，$p_2^{i_2}$阶，…，p_n阶、p_n^2阶，…，$p_n^{i_n}$阶的子群，至于G是否有其他阶的子群（如p_1p_2阶），就不一定了．

一个素数p如果整除群G的阶，那末必有正整数k，使$p^k \mid |G|$，$p^{k+1} \nmid |G|$，p^k是整除$|G|$的最大p方幂．这时，p^k阶子群一定存在，它是一个p群，叫做G的西洛p–子群．

A_4的阶为$12 = 2^2 \cdot 3$，故它含有2阶、4阶、3阶子群．其中4阶子群是西洛2–子群，3阶子群是西洛3–子群．

一个$100 = 2^2 \cdot 5^2$阶群中，西洛2–子群是4阶的，西洛5–子群是25阶的．

有了拉格朗日定理和西洛定理，对于p群的结构就有进一步的了解：

定理5 p群的所有子群是p群．反之，如果$m \leqslant n$，则

p^n 阶 p 群中必有 p^m 阶 p 群。

证明：p^n 的因子也是 p 的方幂，由拉格朗日定理，p 群的子群也是 p 群。

反之，设群 G 的阶为 p^n，$m \leqslant n$，由西洛定理，G 有 P^m 阶子群。

证毕

拉格朗日定理、凯莱定理、西洛定理、有限可换群基本定理以及本节定理 3 常称为有限群五大基本定理。

习 题 3·13

1. 写出 A_4 的两个共轭类.

2. 设 N 是群 G 的子群，求证 N 是正规子群的充要条件是：若 N 含 g，则含 g 的两个共轭元。

3. 求证：群中同一共轭类的元素有相同的阶。

4. 求证：若 a 与 b 共轭，则 a^{-1} 与 b^{-1} 共轭，a^n 与 b^n 共轭 (n 为任意整数)。

5. 设 S 是群 G 的一个共轭类，求证：⟨S⟩是 G 的正规子群。

6. 3200 阶群西洛 2-子群阶为多少?

7. 找出 A_4 的一个西洛 3-子群。

8. 试问：在群⟨$M_2^*(R)$，·⟩中，以下三个方阵是否共轭：$\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$，$\begin{pmatrix}3 & 1\\ 1 & 1\end{pmatrix}$，$\begin{pmatrix}2 & 1\\ -2 & 0\end{pmatrix}$。

9. 求证：p 群的商群也是 p 群。

10. 求证：有限群 G是 p 群的充要条件是它的所有真子群是 p 群。

11. 用西洛定理证明：设 p， q 是不同的素数，pq 阶可换群是循环群。

12. 设素数 p 整除群 G 的阶，求证：G 中存在 p 阶元素。

13. 写出 10 阶群的各种可能的群方程。

*§3·14 可解群与合成群列

可解群是一类重要的群，特别在伽罗华理论中，它起着基本的作用，而它又和合成群列有着密切的关系，后者在剖析有限群的结构时是常用的工具。

一、正规群列

定义 1 设 G 是群，其子群 $G_2,\cdots,G_s$，G_{s+1} 有包含关系

$$G=G_1\supseteq G_2\supseteq\cdots\supseteq G_s\supseteq G_{s+1}=E,\text{注} \tag{1}$$

且每个 G_{i+1} 是 G_i 的正规子群（但不一定是 G 的正规子群），则称 (1) 为 G 的一个正规群列。

显然可换群的任何起于 G 终于 E 的子群包含列都是正规群列。在 S_4 中

$$S_4\supseteq A_4\supseteq B_4\supseteq W\supseteq E$$

$$(W=\{(1),\ (1\ \ 2)(3\ \ 4)\}) \tag{2}$$

显然是正规群列。在 S_3 和 S_2 中，

$$S_3\supseteq A_3\supseteq E,\ \ S_2\supseteq E \tag{3}$$

也都是正规群列。实际上任何群都有正规群列，如 $G\supseteq E$ 就是一个，称为平凡正规群列。

注 约定 E 表示单位元群 $\{e\}$。

每个正规群列(1)都对应一个商群列

$$G_1/G_2,\ G_2/G_3,\ \cdots,\ G_s/G_{s+1}\cong G_s. \qquad (4)$$

二、可解群

定义 2 群 G 如果有一个正规群列(1)，其商群列(4)都是可换群，则称 G 为可解群.

显然可换群是可解群. S_2, S_3, S_4 都是可解群，因为群列(2)(3)中的商群列阶是素数：

$$|S_2/E|=2,\ |S_3/A_3|=2,\ |A_3/E|=3,\ |S_4/A_4|=2,$$
$$|A_4/B_4|=3,\ |B_4/W|=2,\ |W/E|=2,$$

因而是循环群. 可以证明，素数幂阶和奇数阶群都是可解群. 为了给出可解群的判别方法，引进另一个重要概念.

三、换位子与换位子群

定义 3 任取群 G 中元素 a, b，记

$$[a,b]=a^{-1}b^{-1}ab,$$

称为 a,b 的换位子. 群 G 中所有换位子组成的子集 S 所生成的子群，称为 G 的换位子群 G'.

显然，ab 可换当且仅当 $[a,b]=e$；而且 $ab=ba[a,b]$. 所以换位子某种程度上反映了两个元素的可换性.

定理 1 G' 是 G 的正规子群；G/G' 是可换群；若 G/N 是可换群(N 是 G 的正规子群)，则 $G'\subseteq N$.

证明：任取 $g\in G$, $[a,b]\in S$，则

$$\begin{aligned}g[a,b]g^{-1}&=ga^{-1}b^{-1}abg^{-1}\\&=(ga^{-1}g^{-1})(gb^{-1}g^{-1})(gag^{-1})(gbg^{-1})\\&=[gag^{-1},\ gbg^{-1}]\in S.\end{aligned}$$

所以 $gG'g^{-1}\subseteq G'$，G' 是正规子群．设 a，$b\in G$，则

$$aG'\cdot bG'=abG'=ba[a,b]G'=baG'$$
$$=bG'\cdot aG',\ ([a,b]\in G')．$$

所以 G/G' 是可换群．任取 $[a,b]\in S$，

$$[a,b]N=(a^{-1}b^{-1}ab)N=(a^{-1}N)\cdot(b^{-1}N)\cdot(aN)\cdot(bN)．$$

由于 G/N 是可换的，上式化为

$$(a^{-1}N)\cdot(aN)\cdot(b^{-1}N)\cdot(bN)=(a^{-1}a)N\cdot(b^{-1}b)N=N,$$

即 $[a,b]\in N$，$S\subseteq N$，$G'\subseteq N$．

证毕

G 的换位子群 G' 又有换位子群 G''，G'' 又有换位子群 G'''，于是得到一个换位子群列

$$G\supseteq G'\supseteq G''\supseteq G'''\supseteq\cdots \tag{5}$$

定理 2 群 G 可解当且仅当对某个 $k\geqslant 1$，$G^{(k)}=E$．

证明：如果条件成立，则得到正规群列

$$G\supseteq G'\supseteq G''\supseteq\cdots\supseteq G^{(k)}=E,$$

每个 $G^{(i)}/G^{(i+1)}$ 是可换群，因而 G 是可解的．反之，设 G 可解，则有正规群列(1)，每个 G_i/G_{i+1} 是可换群．由定理 1，G_{i+1} 包含 G_i 的换位子群 G_i'．特别 $G_2\supseteq G_1'=G'$，因而，$G_3\supseteq G_2'\supseteq(G')'=G''$，同理 $G_{i+1}\supseteq G^{(i)}$ 对所有 i 成立．因为 $G_{s+1}=E$，于是 $G^{(s)}=E$．

证毕

推论 1 可解群的子群是可解群．

证明：设 H 是可解群 G 的子群，显然 $H^{(i)}\subseteq G^{(i)}$．由定理 2，存在 $k\geqslant 1$，$G^{(k)}=E$．于是 $H^{(k)}=E$，H 是可解群．

推论 2 可解群的商群是可解群．

证明：设 $\bar{G}=G/N$ 是可解群 G 的商群．$[a,b]$ 的同态象

是 a，b 象的换位子；反之，设$[\bar{a},\bar{b}]$是 $\bar{G}$ 的换位子，则有 $a,b\in G$，使 $a\to\bar{a}$，$b\to\bar{b}$，$[a,b]\to[\bar{a},\bar{b}]$，因而$G'$ 在 $\bar{G}$ 中的象正是 $\bar{G}$ 的换位子群．由于 $G^{(k)}=E$，所以在 $\bar{G}$ 中 $\bar{G}^{(k)}=\bar{E}$，即 $\bar{G}$ 是可解群．

证毕

定理 3 $S_n(n\geqslant5)$是不可解群．

证明：假如 S_n 是可解群，设有 S_n 的正规群列(1)，商群列(4)是可换群．S_n 自然包含任意的 3—循环(a,b,c)，另外，任取元素 u，v(异于 a,b,c)，设 $\sigma=(u,b,a)$，$\tau=(a,v,c)$，则由于 G_1/G_2 可换，

$$(\sigma^{-1}\tau^{-1}\sigma\tau)G_2=(\sigma^{-1}G_2)(\tau^{-1}G_2)(\sigma G_2)(\tau G_2)=G_2.$$

即 $\sigma^{-1}\tau^{-1}\sigma\tau\in G_2$．但

$$\begin{aligned}\sigma^{-1}\tau^{-1}\sigma\tau&=(a,b,u)(c,v,a)(u,b,a)(a,v,c)\\&=(a,b,c).\end{aligned}$$

因而 G_2 包含所有 3—循环．同理可知每个 G_i 都包含所有 3-循环，与 $G_{s+1}=E$ 矛盾．

证毕

四、合成群列

一个群如果除平凡子群外无正规子群，则称为单群，如素数阶群是单群．

群G的最大正规子群，是指这样的正规子群 $N(\neq G)$，除了G和N外没有正规子群包含它．如 C_4 是 C_8 的最大正规子群，A_n 是 S_n 的最大正规子群，单群的最大正规子群是 E．

设想在一个有限群G中找出一个最大正规子群G_2，再在

G_2中找出一个最大正规子群G_3；…，最后必然得到正规群列

$$G=G_1\supset G_2\supset\cdots\supset G_{s+1}=E. \tag{6}$$

商群G_i/G_{i+1}一定是单群。因为否则它的非平凡正规子群在G_i中的自然同态原象集也是G的正规子群，介于G_{i+1}与G_i之间，与G_{i+1}最大性矛盾。

定义 4 如果群G的一个形如(6)的正规群列对应的商群都是单群，则(6)称为G的合成群列。s称为群列的长度。

也就是说群的合成群列是最"密"的正规群列。由于方法不同，可能同一个群有几个合成群列。可以证明，它们长度相等，而且他们的商群列适当排列次序后对应同构（约当定理）。

如$\langle a\rangle=C_{12}$，$\langle a\rangle\supset\langle a^2\rangle\supset\langle a^6\rangle\supset\langle a^{12}\rangle=E$和$\langle a\rangle\supset\langle a^3\rangle\supset\langle a^6\rangle\supset\langle a^{12}\rangle=E$都是合成群列，长度都是3，且$\langle a\rangle/\langle a^2\rangle\cong\langle a^3\rangle/\langle a^6\rangle(\cong C_2)$，$\langle a^2\rangle/\langle a^6\rangle\cong\langle a\rangle/\langle a^3\rangle(\cong C_3)$，$\langle a^6\rangle/\langle a^{12}\rangle\cong\langle a^6\rangle/\langle a^{12}\rangle(\cong C_2)$。

群不一定都有合成群列，如无限可换群就没有合成群列，而有限群总有合成群列。

合成群列可以用来判断可解群。

定理 4 有限群是可解群的充要条件是其合成群列的商群列都是素数阶群。

证明：如果G是可解群，由定理2 G有换位子群列：

$$G\supseteq G'\supseteq G''\supseteq\cdots\supseteq G^{(k)}=E.$$

一定有G的一个最大正规子群$G_1\supseteq G'$。所以G/G'与G/G_1同态（映射为$gG'\to gG_1$）。由于G/G'是可换群（定理1），所以其同态象G/G_1也是可换群，又是单群，故一定是素数阶

群。把G_1看成独立的一个群，也是可解群（推论1），同理G_1又有最大子群G_2，G_1/G_2是素数阶群。依次类推，最后必然得到$G_{s+1}=E$。于是，$G \supset G_1 \supset G_2 \supset \cdots \supset G_{s+1}=E$是一个合成群列，相应的商群都是素数阶群。由约当定理，G的任何合成群列都有这一性质。

反之，如果G的合成群列的商群是素数阶群，因而是循环群(可换群)，所以G是可解群。

本 章 提 要

一、群的定义：元素都是可逆元的半群。

二、子群：群的非空子集H是子群当且仅当如果$a,b \in H$，则$ab^{-1} \in H$。

三、陪集：设a是群G的元素，H是子群，aH称为H由a生成的左陪集。相应地，Ha称为右陪集。一般$aH \neq Ha$。左陪集（或右陪集）构成G的分类。左、右陪集与子群等势。

四、正规子群：左陪集与右陪集对应相等的子群。N是正规子群当且仅当对于群中任意a，$aNa^{-1} \subseteq N$。

五、商群：群关于一个正规子群的所有陪集作成的群。

六、群同态基本定理：群关于同态核的商群与同态象同构。

七、有限生成的可换群基本定理：任何有限生成的可换群同构于有限个不可分解循环群的直积。

八、西洛定理：若素数方幂p^k整除群G的阶，则G有p^k阶子群。

复 习 题 三

1．写出五阶以下的群的同构分类．

2．设 u 是群 G 的固定元素，规定 $a\circ b=au^{-1}b$，求证：$\langle G,\circ\rangle$ 是群．

3．设 $G=\{p^m q^n \mid m,\ n\in \mathbf{Z}\}$，其中 p，q 是两个不同的素数，求证 $\langle G,\cdot\rangle$ 是群．

4．设 G 是群，x，$y\in G$，求证：

$$(x^{-1}yx)^k=x^{-1}yx\Longleftrightarrow y^k=y.$$

5．求证：在群中成立 $(a^{-1}ba)^k=a^{-1}b^k a$．

6．设无限群 G 的每个元素的阶有限，且对每一个 $n>0$，G 的 n 阶元素至多有有限个，求证 G 中元素的阶无上界．

7．设 G 是可换群，m 是固定的正整数．求证：

（1）G 中阶为 m 因子的元素作成 G 的子群；

（2）G 中元素的 m 次幂也是 G 的子群．

8．设 G 是可换群，n 是固定自然数，H 表示使方程 $x^n=h$ 有解的元素 h 的集合．求证：H 作成 G 的子群．

9．在 n 阶循环群 $\langle a\rangle$ 中，求证：a^k 的阶等于 $\dfrac{n}{(k,n)}$，其中 (k,n) 表示 k 与 n 的最大公因数．

10．设 G 是可换群，H 是 G 的子群，$a\in G$，$a,a^2,\cdots,a^{n-1}\notin H$，但 $a^n\in H$，假定 a 是有限阶元素，求证：n 是 a 的阶的因子，n 等于商群 G/H 中 aH 的阶．

*11．设 G 是不可换群，C 是它的中心，求证：G/C 不是循环群．由此证明不可换群的自同构群不可能是循环群．

12．设群 G 阶为 n，元素 x 的阶为 m，x 的共轭元共有

k 个，求证 k 整除 $\frac{n}{m}$.

13. 设 n 阶群 G 中的一个共轭类含 k 个元素，G 的中心 C 的阶为 c，求证 k 整除 $\frac{n}{c}$.

*14. 求证：素数平方阶群是可换群.

15. 设 a，x，y 是群 G 的元素，求证：

$$xN(a)=yN(a)\Longleftrightarrow xax^{-1}=yay^{-1}.$$

16. 设 G 与 $\bar{G}$ 同态，则 G 中共轭类的个数不少于 $\bar{G}$ 中共轭类的个数.

*17. 求证：在对称群 S_n 中，元素 $\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ k_1 & k_2 & \cdots & k_n\end{pmatrix}$ 的共轭元形如 $\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma\tau(1) & \sigma\tau(2) & \cdots & \sigma\tau(n)\end{pmatrix}$，其中 $\tau\in S_n$. 由此证明：S_n 的共轭类个数与 n 的不同划分的个数相同；S_n 的中心只有(1)($n>2$).

18. 求证：仅含有限个子群的群的任意满自同态也是自同构.

19. 求证：非单位可换群的自同构群不可能是奇数阶的。假定该群含有高于 2 阶的元素.

*20. 设 $\sigma(g)=g^3$ 是群 G 的单自同态，求证：

(1) $a^2b^2=(ba)^2$；

(2) $a^3b^3=(ba)^3$；

(3) $ab=ba$.($a,b\in G$)

*21. 设群 G 的中心不含非单位元，则其自同构群的中心也不含非恒等变换. 试证明之.

22. 设A和B任意的可换群，A到B的所有同态构成的集合记为$Hom(A,B)$，在其中规定$(\sigma*\tau)(a)=\sigma(a)\cdot\tau(a)$，求证这时$\langle Hom(A,B),*\rangle$是可换群.

23. 设A为C_∞，求证：对于任意可换群B，$Hom(A,B)\cong B$.

24. 求证：$\langle Q,+\rangle$的自同态群同构于自身.

*25. 设B是半群A中可以整除所有元素的元素组成的集合，$B\neq\phi$，求证：B是A的子群.

*26. 设C是半群A中可以被A的所有元素整除的元素组成的集合，$C\neq\phi$，求证：C是A的子群.

*27. 在集合A的变换半群$S(A)$中，求证：

(1) τ是σ的右因子当且仅当由$\tau(\alpha)=\tau(\beta)$推得$\sigma(\alpha)=\sigma(\beta)$；

(2) τ是σ的左因子当且仅当$\sigma[A]\subseteq\tau[A]$.

28. 设p，q是互异的素数，$p<q$. 求证：任意pq阶群有唯一的q阶子群，它是正规子群.

29. 设N_1，N_2是群的两个正规子群，求证：$\langle N_1\cup N_2\rangle$是正规子群，$\langle N_1\cup N_2\rangle=N_1N_2$.

30. 设H_1，H_2，…，是群的子群，且$H_1\subset H_2\subset\cdots$. 求证：如果各$H_i$没有非平凡正规子群，则$\bigcup\limits_{i=1}^{\infty}H_i$也是$G$的这种性质的子群.

31. 求证：一个群不能表为它的两个真子群的并集.

第四章 环

群只有一个代数运算，但通常我们熟悉的代数系如数系、多项式集、矩阵集等却常有两个基本的代数运算，这两个代数运算之间又有密切的关系.

这一章，我们将讨论具有两个代数运算的代数系——环. 主要介绍环、子环、理想、商环、环的同态与同构、整环中的因子分解等基本概念和性质，并讨论一些具体的环.

§4·1 什么是环？

先来看整数系 $\mathbf{Z}$. 我们知道，$\mathbf{Z}$ 关于加法是一个可换群，关于乘法又是一个半群，而乘法关于加法适合分配律. 此外，有理数系 $\mathbf{Q}$、实数系 $\mathbf{R}$、复数系 $\mathbf{C}$ 以及实多项式集 $\mathbf{R}[x]$、实 n 阶方阵集 $M_n(\mathbf{R})$ 等也具有这些性质. 这些代数系的性质加以抽象，可以得到环的概念.

定义1 设 R 是一个非空集合. 它有两个代数运算，分别称为加法和乘法，记为 $+$ 和 $\cdot$. 如果：

(1) $\langle R, +\rangle$ 是可换群；

(2) $\langle R, \cdot\rangle$ 是半群；

(3) 乘法关于加法适合分配律，即对 $a, b, c\in R$，成立

$$a(b+c)=ab+ac,$$

$$(b+c)a=ba+ca,^{注}$$

则称R为环，记为$\langle R,+,\cdot\rangle$．在不会产生误解时，也可记为R．

环中可换群$\langle R,+\rangle$,常称环的加群，其单位元称为环的零元，记为0，元素a的逆元，称为a的负元，记为$-a$。

如果不涉及群和半群，也可以直接给出环的定义：

定义2 设R是一个非空集合，$+$和$\cdot$是R的两个代数运算．如果对任意的a，b，$c\in R$，有

(1) $(a+b)+c=a+(b+c)$；

(2) $a+b=b+a$；

(3) 在R中存在元素0（称为零元），对每个$a\in R$，满足

$$a+0=0+a=a;$$

(4) 对每个$a\in R$，存在负元$-a\in R$，满足

$$a+(-a)=(-a)+a=0;$$

(5) $(ab)c=a(bc)$；

(6) $a(b+c)=ab+bc$，

$(b+c)a=ba+ca$．

则称R是一个环．

注意：其中前4条说明$\langle R,+\rangle$是可换群，第5说明$\langle R,\cdot\rangle$是半群，第6说明乘法关于加法适合分配律．

如上所述，$\langle \mathbf{Z},+,\cdot\rangle$、$\langle \mathbf{Q},+,\cdot\rangle$、$\langle \mathbf{R},+,\cdot\rangle$、$\langle \mathbf{C},+,\cdot\rangle$及一切数环都是环，$\langle \mathbf{R}[x],+,\cdot\rangle$和$\langle M_n(\mathbf{R}),+,\cdot\rangle$也是环．

例1 单元素集$\{0\}$，若规定：$0+0=0$，$0\cdot 0=0$，

注 约定乘法先于加法，如$ab+ac=(ab)+(ac)$．下同．

则作成环，称为零环．其他至少含两个元素的环，称为非零环．

例 2　设 $R=\{0,1\}$，规定：$0+0=0$，$0+1=1+0=1$，$1+1=0$，$0\cdot 0=0\cdot 1=1\cdot 0=0$，$1\cdot 1=1$，则 R 作成环．

事实上，0 是零元，0 是 0 的负元，1 是 1 的负元．易见定义 2 中的各条均能满足，所以 R 是环．

例 3　以 n 为模的剩余类 $\mathbf{Z}_n$，关于 $\mathbf{Z}_n$ 的加法作成加群，关于乘法作成半群．此外，分配律成立：

$$\begin{aligned}[][a]([b]+[c])&=[a][b+c]=[a(b+c)]\\&=[ab+ac]=[ab]+[ac]=[a][b]+[a][c].\end{aligned}$$

同理 $([b]+[c])[a]=[b][a]+[c][a]$.

因而 $\langle \mathbf{Z}_n,+,\cdot\rangle$ 作成环，称为以 n 为模的剩余类环．例 2 实际是例 3 中 $n=2$ 的情况．

由已知环可以造出新的环来，下面的方阵环就是一例：

例 4　设 R 是一个环．由 R 中的元素组成的全体 n 阶方阵的集合，记为 $M_n(R)$：

$$M_n(R)=\left\{\left.\begin{pmatrix}a_{11} & \cdots & a_{1n}\\ \cdots & \cdots & \cdots\\ a_{n1} & \cdots & a_{nn}\end{pmatrix}\right| a_{ij}\in R,\ i,\ j=1,\cdots,n\right\}.$$

在 $M_n(R)$ 中引进类似于数字矩阵的加法与乘法运算．容易验证 $\langle M_n(R),+,\cdot\rangle$ 作成环．称为环 R 上的 n 阶方阵环．

例 5　$\mathbf{Z}$ 中乘法改为规定

$$a*b=a,$$

加法照常，那末 $\langle \mathbf{Z},+,*\rangle$ 是不是环？

解：不是环，因为不适合分配律．如

$$5*(1+1)=5\neq 5+5=(5*1)+(5*1).$$

在这个例子里，$\langle \mathbf{Z}, +\rangle$是可换群，$\langle \mathbf{Z}, *\rangle$是半群，但却不能作成环，因为分配律不成立。所以，环不能仅仅看成可换群与半群的机械的凑合，这两个代数系在环中通过分配律溶为一体。

习　题　4·1

1．以下集合关于数的加法与乘法是否作成环：

(1) n 的全体倍数；　　　　(2) $\mathbf{Z}^+$；

(3) $\{a+b\sqrt{2}\mid a,b\in \mathbf{Z}\}$；　(4) $\{bi\mid b\in \mathbf{R}\}$；

(5) $\left\{\frac{m}{2^n}\middle| m\in \mathbf{Z},\ n\in \mathbf{N}\right\}$.

2．设R是加群，规定 $a*b=0$，求证：$\langle R,+,*\rangle$作成环。

3．设$F[0,1]$表示区间$[0,1]$上全体实函数的集合，求证：$F[0,1]$关于函数的加法与乘法作成环。

4．下表给出的集合$A=\{a,b,c\}$的加法与乘法，是否使A作成环？

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	c

§4·2　环的性质和类型

本节讲述环的基本性质和一些常见类型。

一、基本性质

一个环R，实际上包括了两个代数系：加群$\langle R, +\rangle$与乘半群$\langle R, \cdot\rangle$。两个代数系通过分配律互相联系着。环的每个元素既是加群中的成员，又是乘半群中的成员。那末，加群中的零元、负元，在乘半群中起什么作用呢？

性质1 设0是环R的零元，$a \in R$，则$0 \cdot a = a \cdot 0 = 0$。

证明： $0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$。两端加上$0 \cdot a$的负元，得$0 \cdot a = 0$。

证毕

所以，环的零元也是乘半群的零元（半群的零元概念见§2·3），这一性质是由环的分配律所决定。半群的零元是唯一的，所以乘半群的零元只能是环的零元。

性质2 在环中成立：

(1) $(-a)b = a(-b) = -ab$；

(2) $(-a)(-b) = ab$。

证明： (1) $(-a)b + ab = (-a+a)b = 0 \cdot b = 0$，同理$a(-b) + ab = 0$。

(2) $(-a)(-b) = -a(-b) = ab$。

证毕

性质2说明环中加群的负元在乘半群中的作用。

定义1 加群中规定减法法则如下：

$$a - b = a + (-b)。$$

性质3 在环中成立：

$$c(a-b) = ca - cb，\quad (a-b)c = ac - bc。$$

证明：$c(a-b)+cb=c(a-b+b)=ca$，

$$(a-b)c+bc=(a-b+b)c=ac.$$

性质 4 在环中成立：

$$a(b_1+\cdots+b_n)=ab_1+\cdots+ab_n;$$

$$(b_1+\cdots+b_n)a=b_1a+\cdots+b_na;$$

$$(a_1+\cdots+a_m)(b_1+\cdots+b_n)=a_1b_1+\cdots+a_mb_1+\cdots+a_1b_n+\cdots+a_mb_n.$$

$$(na)b=a(nb)=n(ab)\ (n\text{ 为整数}).$$

证明留给读者.

环的乘半群不一定有单位元，若有单位元，则称为有单位元环. 单位元常记为1（不要与数1相混）. 如$\boldsymbol{Z}$、$\boldsymbol{Z}_n$、$M_n(\boldsymbol{R})$、$\boldsymbol{R}[x]$都有单位元. 除零环外，显然单位元不与零元重合.

二、可换环

环的乘半群不一定可换，如果可换，则称此环为可换环.

如数环、多项式环都是可换环，$\boldsymbol{Z}_n$也是可换环. 但方阵环$M_n(\boldsymbol{R})$不是可换环，如在$M_2(\boldsymbol{R})$中，

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\neq\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

三、无零因子环

我们常把环R的非零元集记为R^*.

对于一般的环，R^*并不关于乘法封闭，因为两个非零元之积可能是零元. 如在$M_2(\boldsymbol{R})$中，

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}\neq 0,\quad \begin{pmatrix}0&0\\0&1\end{pmatrix}\neq 0,$$

但$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$.

又如在环 $\boldsymbol{Z}_6$ 中，$[2]\neq 0$，$[3]\neq 0$，但

$$[2]\cdot[3]=[6]=[0].$$

如果环R的任意非零元的乘积仍是非零元，则$\langle R^*,\cdot\rangle$是$\langle R,\cdot\rangle$的子半群。这种环的意义在哪里呢？

定理1 设R是环，则$\langle R^*,\cdot\rangle$为$\langle R,\cdot\rangle$的子半群的充要条件是成立左消去律，即由 a，b，$c\in R$，$a\neq 0$，$ab=ac$，推出 $b=c$。

证明：若 R^*是R的子半群，$a\neq 0$，$ab=ac$，但 $b\neq c$，则 $b-c\in R^*$，因而 $a(b-c)\in R^*$，$ab-ac=a(b-c)\neq 0$，$ab\neq ac$，推出矛盾。所以 $b=c$。左消去律成立。

若左消去律成立，设 $a,b\in R^*$，即 $a\neq 0$，$b\neq 0$，如果 $ab\bar{\in} R^*$，则 $ab=0=a0$。由左消去律，$b=0$，推出矛盾。所以 $ab\in R^*$。即 R^*是R的子半群。

证毕

定理2 设R是环。则$\langle R^*,\cdot\rangle$为$\langle R,\cdot\rangle$的子半群的充要条件是成立右消去律，即由 $a,b,c\in R$，$a\neq 0$，$ba=ca$，推出 $b=c$。

证明类似定理1。

由定理1和定理2得

推论1 环R中左消去律与右消去律等价。

R^*是环R的子半群也可以从另一个侧面描述。

定义2 设a是环R的非零元，如果存在$b\neq 0$，使ab

$=0$,则称 a 是环 R 的左零因子．如果存在 $b\neq 0$,使 $ba=0$,则称 a 是环 R 的右零因子．对于可换环可以简称为零因子．

既无左零因子又无右零因子的环称为无零因子环．否则，称为有零因子环．

由上所述，$M_2(\mathbf{R})$和 $\mathbf{Z}_6$ 都有零因子．

数环、多项式环都是无零因子环．

例 1 求 $\mathbf{Z}_{10}$ 的所有零因子．

解：设 $[m]$是零因子，则存在 $[k]\neq[0]$，使 $[mk]=[m][k]=[0]$．因而，$10|mk$．但因$[m]\neq[0]$，$10\nmid m$，又 $10\nmid k$,所以 m 只能是：2,4,5,6,8,即$[2]$,$[4]$,$[5]$,$[6]$,$[8]$,是 $\mathbf{Z}_{10}$ 的全部零因子．

除零环外，环的乘半群不会是可消半群,因为有零元(见§2·4 一).但由定理1、2，当 R^*是 R 的子半群时，R^* 是一个可消半群．

一个环若没有零因子，则任取非零元 a，b,可得 $ab\neq 0$,即 R^* 成子半群．反之亦对．这样，我们就得到四个等价的描述方法．即

定理 3 对于环 R，以下断言等价：

(1) R是无零因子环；

(2) $\langle R^*, \cdot\rangle$是$\langle R, \cdot\rangle$的子半群；

(3) R 中成立左消去律或右消去律；

(4) $\langle R^*, \cdot\rangle$是可消半群．

读者可将它们的互推当作练习．

四、整环、体和域

定义 3 无零因子的有单位元的非零可换环,称为整环．

这就是说，整环R的非零元集R^*作成有单位元的可换可消半群.

环R关于乘法不可能成为群（除零环外），但非零元集R^*可以成为群，如$\mathbf{Q}^*$就是乘群.

定义 4 环R中如果$\langle R^*, \cdot\rangle$是群，则$R$称为体，乘法可换的体称为域.

群总是半群，所以体中无零因子.

显然，数域和数域上的有理分式域[注]都是域.

例 2 剩余类环$\mathbf{Z}_n(n>1)$当且仅当n是素数时，是域.

证明： $\mathbf{Z}_n$是有单位元$[1]$的环.

假定n不是素数，设$n=n_1n_2$，$n\nmid n_1$，$n\nmid n_2$，则$[n_1][n_2]=[n_1n_2]=[n]=[0]$. 而$[n_1]\neq[0]$，$[n_2]\neq[0]$，所以$[n_1]$,$[n_2]$是零因子，$\mathbf{Z}_n$自然不是域（因为域无零因子）.

假定n是素数，在$\mathbf{Z}_n$中任取非零元$[k]$，则$n\nmid k$，n与k互素，即有整数u，v，满足

$$un+vk=1.$$

（参见本丛书《多项式代数》附录“整数的整除性”）因而

$$[un]+[vk]=[1].$$

又因$[un]=[0]$，故$[v][k]=[vk]=[1]$. 即$[v]=[k]^{-1}$. 说明非零元是可逆元. 又因乘法的可换性，得知$\langle\mathbf{Z}_n, +, \cdot\rangle$是域.

五、可逆元群

在有单位元的环中，总有可逆元，因为至少单位元就是

注　见本丛书《多项式代数》第七章.

一个．假定环 R 的可逆元集记为 $\bar{R}$，由§3·2定理6，$\langle\bar{R},\cdot\rangle$ 是群．

$\bar{R}$ 称为环 R 的可逆元群，它是乘半群 $\langle R,\cdot\rangle$ 的子群．

除零环外，环 R 的可逆元群 $\bar{R}$ 不包括0，即 $\bar{R}\subseteq R^*$，这是因为0不可逆（§2·2定理5）．对于体（包括域），$\bar{R}$ 充满了整个 R^*．

环的结构如图4—1所示．其中 R——环，R^*——非零元集，$\bar{R}$——可逆元集，Z——左、右零因子集，1——单位元，0——零元．由定理3，$Z\cap\bar{R}=\phi$，但 $Z\subseteq R^*$，$1\in\bar{R}\subseteq R^*$，又 $R=R^*\cup\{0\}$．

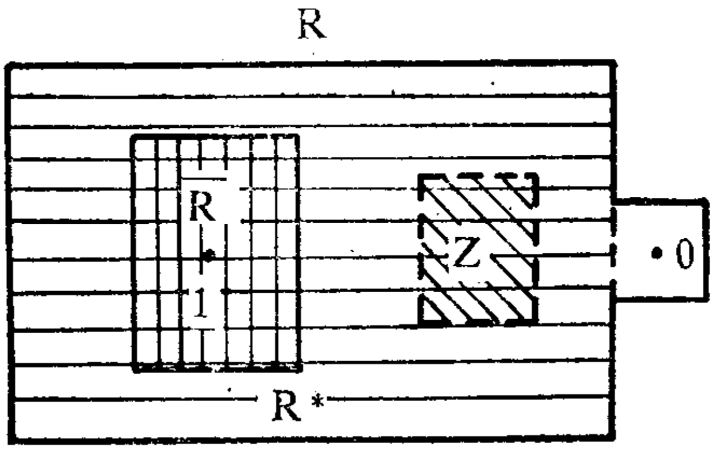


图4—1

整数环 $\boldsymbol{Z}$ 的可逆元群是 $\{1,-1\}$．

$M_n(\boldsymbol{R})$ 的可逆元群由一切 n 阶实非退化方阵组成．

例3 分析 $\boldsymbol{Z}_n$ 的可逆元群．

解：设 $[k]\in\boldsymbol{Z}_n$ 是可逆元，则存在 $[h]\in\boldsymbol{Z}_n$，使 $[hk]=[h][k]=[1]$．因而 $n\mid kh-1$．即存在整数 u，使 $kh-1=nu$，即 $kh-nu=1$，因而 k 与 n 互素．

反之，设 k 与 n 互素，则存在整数 u，v，使 $uk+vn=1$，所以

$$[u][k]=[uk]=[1-vn]=[1],$$

即$[k]^{-1}=[u]$。

若k与n互素，则$[k]$中的所有整数与n互素。事实上，若$k_1\in[k]$但与n不互素，设$k_1=qn+k$，则$k=k_1-qn$也不与n互素。

所以，$\mathbf{Z}_n$的可逆元群包括全体这样的剩余类：$[k]$，其中$1\leq k<n$，k与n互素。由§3·11例1知，这样的k共有$\varphi(n)$个（φ——欧拉函数），即$\mathbf{Z}_n$的可逆元群阶为$\varphi(n)$。如$\mathbf{Z}_4$有$\varphi(4)=2$个可逆元：$[1]$，$[3]$；$\mathbf{Z}_6$有$\varphi(6)=2$个可逆元：$[1]$，$[5]$；$\mathbf{Z}_{10}$有$\varphi(10)=4$个可逆元：$[1]$，$[3]$，$[7]$，$[9]$。

由此易得数论中著名的欧拉一费马（Euler—Fermat）定理：注

定理4 设正整数a与n互素，则$a^{\varphi(n)}\equiv 1 \pmod n$。

注意：$a\equiv b\pmod n$表示a与b关于n同余，即$n\mid a-b$，见§1·3例7。

证明：由于a与n互素，故$[a]$属于$\mathbf{Z}_n$的可逆元群$\bar{R}_n$。而$|\bar{R}_n|=\varphi(n)$，由§3·4三，

$$[a]^{\varphi(n)}=[1],$$

$$[a^{\varphi(n)}]=\overbrace{[a]\cdots[a]}^{\varphi(n)\text{个}}=[a]^{\varphi(n)}=[1].$$

即
$$a^{\varphi(n)}\equiv 1\pmod n.$$

证毕

例4 高斯数环$\mathbf{Z}[i]$的可逆元群包括哪些元素？注

解：设$a+bi$是可逆元，那末

注 P. Fermat(1601—1665)，法国数学家。

注 $\mathbf{Z}[i]=\{a+bi\mid a,\ b\in\mathbf{Z}\}$称为高斯数环。

$$\frac{1}{a+bi}=\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\in \mathbf{Z}[i].$$

即$\frac{a}{a^2+b^2}$，$\frac{b}{a^2+b^2}$是整数．因为 a ,b 不全为零，设 $a\neq 0$，则 $b=0$，否则 $0<\left|\frac{a}{a^2+b^2}\right|<1$．$\frac{a}{a^2+b^2}=\frac{a}{a^2}=\frac{1}{a}$是整数，所以 $a=\pm 1$，$a+bi=\pm 1$．同理，若 $b\neq 0$，必有 $a+bi=\pm i$．反之，易见 ± 1 和 $\pm i$ 都是可逆元．故 $\mathbf{Z}[i]$ 的可逆元群是 $\{1,-1,i,-i\}=U_4$(4 次单位根群)．

习　题　4·2

1．找出 $\mathbf{Z}_{20}$ 的可逆元与零因子．

2．找出 $\mathbf{Z}_{24}$ 的可逆元与零因子．

3．实函数环 $F[0,1]$(见习题 4·1)是否整环？

4．求证：整环中除 0 和 1 外没有幂等元(满足 $x^2=x$ 的元素)，除 0 外没有幂零元（对某个 n 满足 $x^n=0$ 的元素)．

5．若 a 是环的非零元素，存在 $b\neq 0$ 使 $aba=0$，求证：a 是左零因子或右零因子．

6．以下剩余类环中哪些是域？

$$\mathbf{Z}_2,\ \mathbf{Z}_4,\ \mathbf{Z}_{11},\ \mathbf{Z}_{17},\ \mathbf{Z}_{51},\ \mathbf{Z}_{101},\ \mathbf{Z}_{471}.$$

7．证明本节性质 4．

8．设环 R 无零因子，求证：$\langle R,+\rangle$ 中非零元阶数相同．

9．习题 4·1 第 1 (5)题的环中可逆元有哪些？

10．求证：环的左（右）零因子不是可逆元．

11．求证：有限非零整环是域．

12．求$[24]$在 $\mathbf{Z}_{29}$ 中的逆元．

13. 设 p 是素数，p 不整除 a，求证：$a^{p-1}-1$ 是 p 的倍数。

14. 设环 R 的加群是循环群，求证：R 是可换环。

15. 求证：$\mathbf{Z}_n$ 的零因子包括一切 $[k]$，其中 k 与 n 不互素。

16. 在 $\mathbf{Z}$ 中规定 $a\oplus b=a+b-1$，$a\odot b=a+b-ab$，求证：$\langle \mathbf{Z},\oplus,\odot\rangle$ 是环，单位元是 0，零元是 1，且没有零因子，可逆元为 0 和 2。

17. 求证：数域及数域上的有理分式域是域。

§4·3 子环与理想

在群里的子群、正规子群相当于环里的子环、理想，许多性质都是相互对应的。本节介绍子环、理想的概念。

一、子环

定义 1 环 R 的非空子集 S，如果关于 R 的加法和乘法也作成环，则称 S 为 R 的子环，也称 R 为 S 的扩环。

S 为 R 的子环，等价于说，$\langle S,+\rangle$ 是 $\langle R,+\rangle$ 的子群，且 $\langle S,\cdot\rangle$ 是 $\langle R,\cdot\rangle$ 的子半群。

如整数环是有理数域的子环，偶数环是整数环的子环。

任意环都有子环，因为环 R 和 $\{0\}$ 显然都是 R 的子环，称为环 R 的平凡子环，其他子环称为真子环。

判断环的子集是否子环常用以下方法：

定理 1 环 R 的非空子集 S 是 R 的子环的充要条件是 S 关于减法和乘法封闭，即

(1) 如果 $a,b\in S$，则 $a-b\in S$；

(2) 如果 $a,b\in S$，则 $ab\in S$。

证明：必要性显然，只须证明充分性。

由§3·3定理2，$\langle S,+\rangle$是$\langle R,+\rangle$的子群。又由§2·1，$\langle S,\cdot\rangle$是$\langle R,\cdot\rangle$的子半群。分配律自然满足。所以，S作成R的子环。

证毕

例1 由$D_n(\mathbf{R})$表示实n阶对角方阵的全体。由于对角方阵的差与积仍是对角方阵，由定理1知，$D_n(\mathbf{R})$是$M_n(\mathbf{R})$的子环。

例2 找出$\mathbf{Z}_6$的所有子环。

解：$\mathbf{Z}_6$的子环显然是$\langle \mathbf{Z}_6,+\rangle$的子群。$\langle \mathbf{Z}_6,+\rangle$是循环群，生成元为[1]，其子群有

$$\{[0]\},\{[0],[3]\},\{[0],[2],[4]\},\mathbf{Z}_6.$$

它们都关于乘法封闭，因而是$\mathbf{Z}_6$的全部子环。

二、理想

理想，是一类特殊的子环，它在环的理论中起着极为重要的作用。先从一个具体例子说起：

设n是一个正整数，n的全体倍数组成的集合，记为$\langle n\rangle$。显然$\langle n\rangle$是$\mathbf{Z}$的子环。任取$a\in\mathbf{Z},k\in\langle n\rangle$，则$ak$仍是$n$的倍数，即$ak\in\langle n\rangle$。$\langle n\rangle$这个子环，具有比一般子环更强的"封闭性"，即$\mathbf{Z}$中任意两个元素中只要有一个属于$\langle n\rangle$，其积就一定属于$\langle n\rangle$。一般地，有

定义2 设I是环R的子环，如果对于任意的$r\in R$和$a\in I$，都有$ar\in I$，$ra\in I$，则称I是R的理想子环，简称

理想。

任何环都有理想，例如平凡子环都是理想，称为平凡理想。其中$\{0\}$称为零理想，环本身称为单位理想，其他理想称真理想。

定理 2 环R的非空子集I为理想的充要条件为：

(1) 如果$a,b\in I$，则$a-b\in I$；

(2) 如果$a\in I$，$b\in R$，则$ab\in I$，$ba\in I$。

证明留作练习。

并非所有环都有真理想，例如体(因而域)没有真理想。事实上，设S是体P的非零理想，设$0\neq a\in S, 1=aa^{-1}\in S$，任取$p\in P$，则$p=1\cdot p\in S$，所以$S=P$是单位理想。

例 3 写出$\boldsymbol{Z}_6$的所有理想。

解：不难验证其四个子环都是理想。

环里的已知理想还可以生成新的理想。

定理 3 环R的任意理想的交也是理想。

证明：设$I_j, j\in J$(J——指标集)是环R的理想。$0\in\bigcap\limits_{j\in J}I_j\neq\phi$。任取$x$，$y\in\bigcap\limits_{j\in J}I_j$，由于$I_j$是理想，故$x-y\in I_j$，($j\in J$)。从而$x-y\in\bigcap\limits_{j\in J}I_j$。

任取$x\in\bigcap\limits_{j\in J}I_j$，$r\in R$，则由于$xr\in I_j$，$rx\in I_j(j\in J)$，从而$xr\in\bigcap\limits_{j\in J}I_j$，$rx\in\bigcap\limits_{j\in J}I_j$。

根据定理 2，$\bigcap\limits_{j\in J}I_j$是$R$的理想。

证毕

三、理想的生成元

设R是环，$S\subseteq R$。包含S的理想总存在，如R就是一个。由定理3，包含S的所有理想之交是R的理想。这个理想称为S生成的理想，记为$\langle S\rangle$，也可以说，$\langle S\rangle$是含S的最小理想。

由已知集合S找出它所生成的理想$\langle S\rangle$，并不是容易的事情。下面只讨论两种基本情况。

1. S是单元集$\{a\}$。

这时，理想$\langle a\rangle$称为由a生成的主理想。设I是含a的任一理想。首先，$ma\in I(m\in\mathbf{Z})$。此外，对于$r,s\in R$，总有$ra,as,ras\in I$。因而I应包含上面形式的有限和：

$$r_1as_1+\cdots+r_tas_t+ra+as+ma. \tag{1}$$

另一方面，显然(1)形的所有元素组成的集合A是一个理想。所以$\langle a\rangle=A$。

对于有单位元的可换环，主理想将更简单。这时(1)形元素可化为$(r_1s_1+\cdots+r_ts_t+r+s)a+ma$。设括号的元素为$\bar{r}$，而$ma=(m\cdot1)a$，所以(1)形元素化为$\bar{r}a+(m\cdot1)a=(\bar{r}+m\cdot1)a=ra$，其中$r=\bar{r}+m\cdot1\in R$(1是$R$的单位元)。所以这时主理想$\langle a\rangle$的元素形如$ra(r\in R)$。如$\mathbf{Z}$中$\langle m\rangle=\{km\mid k\in\mathbf{Z}\}$，$\mathbf{R}[x]$中$\langle f(x)\rangle=\{f(x)g(x)\mid g(x)\in\mathbf{R}[x]\}$。

2. S是有限集$\{a_1,a_2,\cdots,a_n\}$。

首先，形如

$$s_1+s_2+\cdots+s_n,\ (s_1\in\langle a_1\rangle,\cdots,s_n\in\langle a_n\rangle) \tag{2}$$

的元素在包含S的任一理想中；另外，(2)形的元素之差以及(2)形元素与R中元素r之积显然也是(2)形。所以，全体

(2)形的元素组成的集合作成包含 S 的最小理想．即

$$\langle S\rangle=\langle a_1,\cdots,a_n\rangle$$
$$=\{s_1+\cdots+s_n \mid s_1\in\langle a_1\rangle,\cdots,s_n\in\langle a_n\rangle\}. \qquad (3)$$

也可写作

$$\langle a_1,\cdots,a_n\rangle=\langle a_1\rangle+\cdots+\langle a_n\rangle.$$

例 4 $\mathbf{Z}$ 中 $\langle 4,10\rangle$ 包含哪些元素？

解： 由(3)，$\langle 4,10\rangle=\{a+b \mid a\in\langle 4\rangle, b\in\langle 10\rangle\}$

$$=\{4k+10l \mid k,l\in\mathbf{Z}\}.$$

$4k+10l$ 是偶数，反之任一偶数 $2t$ 可以写成

$$2t=4\cdot(-2t)+10t\in\langle 4,10\rangle.$$

所以，$\langle 4,10\rangle=\langle 2\rangle$．

2 是 4 和 10 的最大公因数．一般说来，如果 d 是 m 和 n 的最大公因数，则 $\langle m,n\rangle=\langle d\rangle$．

事实上，由最大公因数的性质，存在 $u,v\in\mathbf{Z}$，使 $d=mu+nv\in\langle m\rangle+\langle n\rangle=\langle m,n\rangle$，故 $\langle d\rangle\subseteq\langle m,n\rangle$．反之，$\langle m,n\rangle$ 中元素形如 $mk+nl(k,l\in\mathbf{Z})$ 是 d 的倍数，即 $\langle m,n\rangle\subseteq\langle d\rangle$．总之，$\langle m,n\rangle=\langle d\rangle$．

同一个主理想 $\langle a\rangle$ 的生成元不一定只有 a，如在 $\mathbf{Z}$ 中，$\langle 2\rangle=\langle -2\rangle$．在整环中，显然 $\langle a\rangle=\langle b\rangle$ 当且仅当 a 与 b 相伴（见§2·3）．

习 题 4·3

1．设 I 是环 R 的理想，$1\in I$，求证 $I=R$．

2．设 I 是环 R 的理想，I 中含有可逆元，求证 $I=R$．

3．求证：子环的交也是子环，子域的交也是子域．

4．设 R 是可换环，$a\in R$，$I_a=\{x\in R \mid ax=0\}$，求证 I_a

是 R 的理想。

5. 找出 $\mathbf{Z}_{12}$ 的所有理想。

6. 设 R 是可换环，求证：R 的全体幂零元(见习题 4·2)作成 R 的理想。

7. 环 $M_2(\mathbf{Z})$ 中由 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ 生成的主理想是什么？

*8. 求证：整数环的所有理想是主理想。

9. 在$\mathbf{R}[x]$中，求证：

(1) $\langle x^2-1\rangle \cap \langle (x+1)^2\rangle = \langle (x+1)^2(x-1)\rangle$；

(2) $\langle x^2-1,(x+1)^2\rangle = \langle x+1\rangle$。

10. 设 R 是整环，每个元素满足 $r^2=r$，求证：$|R|=2$。

*11. 设 $I_1\subseteq I_2\subseteq I_3\subseteq\cdots$ 是环的理想包含链，求证：$\bigcup_{n=1}^{\infty} I_n = I$ 是 R 的理想。

12. 设 + 和 · 是集合 S 的代数运算，满足：

(1) $\langle S,+\rangle$是群；

(2) $\langle S^*,\cdot\rangle$是群，其中 S^* 表示 S 除了加群单位元 0 之外的元素集合；

(3) 乘法关于加法有分配律成立。

求证：$\langle S,+,\cdot\rangle$是体。

13. 证明定理 2 。

§ 4·4 商环与环的同态

上一章，我们看到，群的每个子群可以决定一系列陪集，特别当这个子群是正规子群时，全体陪集按陪集的乘法

作成商群。现在，我们对环作类似的讨论。

一、从理想到商环

设 I 是环 R 的理想，I 自然也是 R 的子环，$\langle I,+\rangle$ 是 $\langle R,+\rangle$ 的子群。加群是可换群，所以 $\langle I,+\rangle$ 是 $\langle R,+\rangle$ 的正规子群。由 $\langle I,+\rangle$ 得到 $\langle R,+\rangle$ 的陪集：

$$a+I,b+I,c+I,\cdots$$

它们作成 $\langle R,+\rangle$ 的商群 $\langle R/I,+\rangle$.其加法为：

$$(a+I)+(b+I)=(a+b)+I。\qquad (1)$$

在 R/I 中引入一个新的法则：

$$(a+I)(b+I)=ab+I。\qquad (2)$$

引理 1 设环 R 有理想 I，则法则(2)是商集合 R/I 的代数运算。

分析：只须证明法则(2)与陪集的代表元选取无关，即结果是唯一的。

证明：如果 $a+I=a_1+I$，$b+I=b_1+I$，则 $a-a_1=i_1\in I,b-b_1=i_2\in I$。

$$a=a_1+i_1,\quad b=b_1+i_2,$$

$$ab=a_1b_1+i_1b_1+ai_2+i_1i_2。$$

由于 I 是理想，故 $i_1b,ai_2,i_1i_2\in I$，因而 $i_1b_1+ai_2+i_1i_2\in I$，$ab\in a_1b_1+I$，故

$$ab+I=a_1b_1+I。$$

证毕

以后约定，法则(2)称为商集合 R/I 的乘法。即 a 所在陪集与 b 所在的陪集之积等于 ab 所在的陪集。

注意：如果 A 是非理想的子环，那末 $\langle A,+\rangle$ 虽是 $\langle R,+\rangle$

的子群，但法则(2)不是商集合的代数运算．如 $\mathbf{Z}$ 是 $\mathbf{Q}$ 的子环，按法则(2)，

$$\left(\frac{1}{2}+\mathbf{Z}\right)\cdot\left(\frac{1}{3}+\mathbf{Z}\right)=\frac{1}{6}+\mathbf{Z}.$$

而 $\frac{1}{2}+\mathbf{Z}=\frac{3}{2}+\mathbf{Z}$，由(2)，又有

$$\left(\frac{3}{2}+\mathbf{Z}\right)\cdot\left(\frac{1}{3}+\mathbf{Z}\right)=\frac{1}{2}+\mathbf{Z}.$$

但 $\frac{1}{6}+\mathbf{Z}\neq\frac{1}{2}+\mathbf{Z}\left(\frac{1}{6}-\frac{1}{2}\overline{\in}\mathbf{Z}\right)$，破坏了代数运算的唯一性．原因在于 $\mathbf{Z}$ 不是 $\mathbf{Q}$ 的理想．

定理 1 设 I 是环 R 的理想，则商集合按加法（1）和乘法(2)作成环 $\langle R/I,+,\cdot\rangle$．

证明：我们已经知道 $\langle R/I,+\rangle$ 是加群．

由引理 1，$\langle R/I,\cdot\rangle$ 是群胚．又因

$$\begin{aligned}&[(a+I)(b+I)](c+I)\\=&(ab+I)(c+I)\\=&(ab)c+I\\=&a(bc)+I\\=&(a+I)(bc+I)\\=&(a+I)[(b+I)(c+I)].\end{aligned}$$

所以，乘法适合结合律．

$$\begin{aligned}&(a+I)[(b+I)+(c+I)]\\=&(a+I)[(b+c)+I]\\=&a(b+c)+I\\=&(ab+ac)+I\\=&(ab+I)+(ac+I)\end{aligned}$$

$$=(a+I)(b+I)+(a+I)(c+I).$$

同理，$[(b+I)+(c+I)](a+I)=(b+I)(a+I)+(c+I)\cdot(a+I)$.分配律成立.

总之，$\langle R/I,+,\cdot\rangle$是环.

证毕

定义1 $\langle R/I,+,\cdot\rangle$称为环$R$关于理想$I$的商环.

例1 设n是正整数，$\mathbf{Z}$关于理想$\langle n\rangle$的商环$\mathbf{Z}/\langle n\rangle$包括$\langle n\rangle,1+\langle n\rangle,\cdots,n-1+\langle n\rangle$. 即

$$\mathbf{Z}/\langle n\rangle=\{[0],[1],\cdots,[n-1]\}=\mathbf{Z}_n.$$

例2 高斯数环$\mathbf{Z}[i]$关于主理想$\langle 2+i\rangle$的商环包含哪些元素？

解：$\mathbf{Z}[i]$是整环，所以$\langle 2+i\rangle$的元素形如$(2+i)(a+bi)$，其中a，b是任意整数.

任取$x+yi\in\mathbf{Z}[i]$，则

$$\begin{aligned}x+yi&=x-2y+y(2+i)\\&=t+5k+y(2+i)\\&=t+k(2-i)(2+i)+y(2+i)\\&=t+[k(2-i)+y](2+i)\in t+\langle 2+i\rangle,\end{aligned}$$

这里$x-2y=t+5k$，$t=0,1,2,3,4$，t由x和y唯一决定，它是$x-2y$被5除的余数. 这就是说$\mathbf{Z}[i]$中的每个元素属于$\langle 2+i\rangle,1+\langle 2+i\rangle,2+\langle 2+i\rangle,3+\langle 2+i\rangle,4+\langle 2+i\rangle$中之一. 显然以上5个陪集互不相同. 所以它们是$\mathbf{Z}[i]/\langle 2+i\rangle$的全部元素.

例3 由上节例3，$I_2=\{[0],[3]\}$是$\mathbf{Z}_6$的理想. $\mathbf{Z}_6/I_2=\{I_2,[1]+I_2,[2]+I_2\}$. 下面写出它的加法表和乘法表：

+	$[1]+I_2$	$[2]+I_2$	I_2
$[1]+I_2$	$[2]+I_2$	I_2	$[1]+I_2$
$[2]+I_2$	I_2	$[1]+I_2$	$[2]+I_2$
I_2	$[1]+I_2$	$[2]+I_2$	I_2

$\cdot$	$[1]+I_2$	$[2]+I_2$	I_2
$[1]+I_2$	$[1]+I_2$	$[2]+I_2$	I_2
$[2]+I_2$	$[2]+I_2$	$[1]+I_2$	I_2
I_2	I_2	I_2	I_2

二、同态与同构

设σ是环R到环$\bar{R}$的映射，为了简便，两个环的代数运算用同样的记号+和·表示。如果σ既是$\langle R,+\rangle$到$\langle \bar{R},+\rangle$的同态，又是$\langle R,\cdot\rangle$到$\langle \bar{R},\cdot\rangle$的同态，则称$\sigma$是环$R$到$\bar{R}$的同态。如果有环$R$到环$\bar{R}$的同态满射，则称环$R$与环$\bar{R}$同态。如果环同态映射$\sigma$同时是一一映射，则称$\sigma$是环$R$到环$\bar{R}$的同构，这时称环$R$与环$\bar{R}$同构，记为$R\cong\bar{R}$。

例 4 求证：环$\mathbf{Z}$与环$\mathbf{Z}_n$同态。

证明：取$\mathbf{Z}$到$\mathbf{Z}_n$的映射σ为

$$\sigma(a)=[a],(a\in\mathbf{Z}).$$

σ显然是满射。又因

$$\sigma(a+b)=[a+b]=[a]+[b]=\sigma(a)+\sigma(b),$$

$$\sigma(ab)=[ab]=[a][b]=\sigma(a)\sigma(b),$$

故σ是同态，$\mathbf{Z}$与$\mathbf{Z}_n$同态。

三、同态基本定理

定理 2 设 σ 是环 R 到环 $\bar{R}$ 的同态，则

(1) 同态核

$$K_\sigma=\{r\in R\mid\sigma(r)=\bar{0}\}$$

是 R 的理想；

(2) R 的象集 $\sigma[R]$ 是 $\bar{R}$ 的子环。

证明：σ 是环 R 到环 $\bar{R}$ 的同态，自然也是加群 $\langle R,+\rangle$ 到 $\langle\bar{R},+\rangle$ 的同态。由 § 3·9 定理 2，K_σ 是 $\langle R,+\rangle$ 的（正规）子群。任取 $k\in K_\sigma$，$r\in R$，则 $\sigma(kr)=\sigma(k)\sigma(r)=\bar{0}$。所以 $kr\in K_\sigma$。类似可证 $rk\in K_\sigma$。所以 K_σ 是 R 的理想。

设 $\sigma(a),\sigma(b)\in\sigma[R]$，则

$$\sigma(a)-\sigma(b)=\sigma(a-b)\in\sigma[R],$$

$$\sigma(a)\sigma(b)=\sigma(ab)\in\sigma[R].$$

由 § 4·3 定理 1，$\sigma[R]$ 是 $\bar{R}$ 的子环。

证毕

从这里我们看出，理想在环中与正规子群在群中起着同样的作用，由环同态决定一个理想，而理想决定一个商环．反过来，由商环也决定一个同态，这就是

定理 3 设 I 是环 R 的理想，那末 R 与商环 R/I 同态．

证明：让 R 的每个元素映射为它所在的陪集．即 $\sigma(r)=r+I$，$(r\in R)$。σ 称为自然同态。

σ 显然是满射．又由于

$$\begin{aligned}\sigma(r_1+r_2)&=(r_1+r_2)+I\\&=(r_1+I)+(r_2+I)\\&=\sigma(r_1)+\sigma(r_2).\end{aligned}$$

$$\sigma(r_1\cdot r_2)=r_1r_2+I$$
$$=(r_1+I)(r_2+I)$$
$$=\sigma(r_1)\cdot\sigma(r_2).$$

所以，σ 是同态满射，即 R 与 R/I 同态。

证毕

如同群的情况一样，环的同态也可以造成一个同构，这就是

定理 4 （环同态基本定理）设 σ 是环 R 到环 $\bar{R}$ 的同态，则

$$R/K_\sigma\cong\sigma[R].$$

证明：将 R，$\bar{R}$ 先看作加群，那末 σ 也是加群的同态。由群同态基本定理，

$$\langle R/K_\sigma,+\rangle\cong\langle\sigma[R],+\rangle.$$

其同构映射为：

$$r+K_\sigma\to\sigma(r). \tag{3}$$

下面证明上述映射也是商环 R/K_σ 到环 $\sigma[R]$ 的同构。为此，只须证明映射(3)关于乘法也是同态的。事实上，任取 $r+K_\sigma, s+K_\sigma\in R/K_\sigma$，则

$$(r+K_\sigma)(s+K_\sigma)=rs+K_\sigma$$
$$\to\sigma(rs)=\sigma(r)\sigma(s).$$

证毕

如果把同构的环不加区分，那末从定理 3 和定理 4 可以看出，环的同态象是且仅是这个环的商环。一个环的所有商环，就是在同构意义下环的所有同态象。

例 5　求证：$\mathbf{Z}_6/I_2\cong\mathbf{Z}_3$.

证明：建立 $\mathbf{Z}_6$ 到 $\mathbf{Z}_3$ 的映射如下：

$$\sigma([0])=\sigma([3])=[0]\in \mathbf{Z}_3,$$
$$\sigma([1])=\sigma([4])=[1]\in \mathbf{Z}_3,$$
$$\sigma([2])=\sigma([5])=[2]\in \mathbf{Z}_3.$$

易见σ是环同态．其核是$I_2=\{[0],[3]\}$．由同态基本定理．$\mathbf{Z}_6/I_2\cong \mathbf{Z}_3$．

上述结果也可以直接验证．作出$\mathbf{Z}_3$的运算表，与例3所示的表对照，令$I_2\to[0]$，$[1]+I_2\to[1]$，$[2]+I_2\to[2]$，则运算完全一致．

+	[1]	[2]	[0]
[1]	[2]	[0]	[1]
[2]	[0]	[1]	[2]
[0]	[1]	[2]	[0]

•	[1]	[2]	[0]
[1]	[1]	[2]	[0]
[2]	[2]	[1]	[0]
[0]	[0]	[0]	[0]

推论1 设σ是环R到环$\bar{R}$的满同态，则
$$R/K_\sigma\cong\bar{R}.$$

推论2 设σ是环R到环$\bar{R}$的满同态，则σ是同构的充要条件是$K_\sigma=\{0\}$．

证明：如果σ是同构，则σ是一一映射．因$\bar{0}$的原象唯一，即$k_\sigma=\{0\}$．

反之，如果$K_\sigma=\{0\}$，则
$$\bar{R}\cong R/K_\sigma=R/\{0\}\cong R.$$

证毕．

四、同态的性质

如果环R与$\bar{R}$同态，R的许多性质可以转移到$\bar{R}$上来．如R的零元的象是$\bar{R}$的零元，R中元素a的负元$-a$的象是

a 的象的负元。R 如有单位元 1，则 1 的象是 $\bar{R}$ 的单位元。R 如果可换，则 $\bar{R}$ 也可换。这些性质请读者自证。

但有无零因子这一性质却不能转移到同态象中去。

如 $\mathbf{Z}$ 没有零因子，$\mathbf{Z}$ 与 $\mathbf{Z}_4$ 同态，但 $\mathbf{Z}_4$ 有零因子[2]([2][2]=[0])。

又如 $\mathbf{Z}_6$ 与 $\mathbf{Z}_3$ 同态，$\mathbf{Z}_6$ 有零因子 [2]，[3]([2][3]=[0])，但 $\mathbf{Z}_3$ 无零因子。

只要两个环同构，则运算的代数性质完全相同。

下面考查同态下两个环的子环与理想的对应关系，它类似于群同态下子群与正规子群的对应关系（§3·10）。

定理 5 设环 R 与 $\bar{R}$ 同态，则

(1) R 中子环(或理想)的象集是 $\bar{R}$ 的子环(或理想)；

(2) $\bar{R}$ 的子环（或理想）的原象集是 R 的子环（或理想）。

证明留作练习。

类似于群的情况，也有

定理 6 （环第一同构定理）设 σ 是环 R 到环 $\bar{R}$ 的满同态，$\bar{I}$ 是 $\bar{R}$ 的理想，$I=\sigma^{-1}[\bar{I}]$，则 $R/I\cong\bar{R}/\bar{I}$。

证明：作 R 到 $\bar{R}/\bar{I}$ 的映射 τ 如下：

$$\tau(r)=\sigma(r)+\bar{I},(r\in R)$$

即 τ 将 r 变为 $\sigma(r)$ 所在的陪集。

τ 是满射。事实上，任取 $\bar{r}+\bar{I}\in\bar{R}/\bar{I}$，由于 σ 是满射，故有 $r\in R$，使 $\sigma(r)=\bar{r}$。

$$\tau(r)=\sigma(r)+\bar{I}=\bar{r}+\bar{I}.$$

τ 是同态。事实上，显然，τ 是加群同态，其次，

$$\tau(r_1r_2)=\sigma(r_1r_2)+\bar{I}$$

$$
\begin{aligned}
&= \sigma(r_1)\sigma(r_2) + \bar{I} \\
&= [\sigma(r_1) + \bar{I}][\sigma(r_2) + \bar{I}] \\
&= \tau(r_1)\tau(r_2).
\end{aligned}
$$

τ 的核 $K_\tau = \{r \mid \tau(r) = \bar{I}\} = \{r \mid \sigma(r) \in \bar{I}\} = I$.

所以，$R/I \cong \bar{R}/\bar{I}$.

证毕

例 6　设 $\mathbf{Z}$ 到 $\mathbf{Z}_6$ 的自然同态为 σ，$I_2 = \{[0],[3]\}$ 是 $\mathbf{Z}_6$ 的理想，其逆象集包括 6 的倍数及用 6 除余 3 的整数，即全体 3 的倍数，于是 $\sigma^{-1}[I_2] = \langle 3 \rangle$。由第一同构定理，得到

$$(\mathbf{Z}_3 =)\mathbf{Z}/\langle 3 \rangle \cong \mathbf{Z}_6/I_2.$$

与例 5 结果相同。

五、自同态与自同构

环 R 到自身的同态映射（不一定是满同态）简称自同态。环 R 到自身的同构映射，也称自同构。

例 7　试求整数环 $\mathbf{Z}$ 的所有自同态和自同构。

解：环 $\mathbf{Z}$ 的自同态 σ，首先是 $\langle \mathbf{Z}, + \rangle$ 的自同态，因而由 §2·4 例 3 知，一定存在 $p \in \mathbf{Z}$，使对于 $a \in \mathbf{Z}$，

$$\sigma(a) = pa, \tag{4}$$

如果 $p = 0$，显然(4)是一个自同态。

如果 $p \neq 0, \sigma(4) = 4p$，$\sigma(2)\sigma(2) = 2p \cdot 2p = 4p^2$，所以 $4p = 4p^2$，$p = 1$。这时 σ 是恒等变换。

因而 $\mathbf{Z}$ 只有两个自同态：零自同态与恒等自同态，后者是唯一的自同构。

例 8　试求高斯数环的所有自同构。

解：$\mathbf{Z}[i]$ 是一个有单位元环。设 σ 是自同构，则 $\sigma(1)$

$=1$，$\sigma(2)=\sigma(1+1)=\sigma(1)+\sigma(1)=2$，$\sigma(0)=0$，$\sigma(-2)$ $=-\sigma(2)=-2$，同理可知，所有整数是 σ 的不变元.

设 $\sigma(i)=a+bi$。$\sigma(i^2)=\sigma(-1)=-1$，但

$$\sigma(i^2)=\sigma(i)\sigma(i)=(a+bi)^2=a^2+2abi-b^2.$$

所以 $$a^2-b^2=-1,\ 2ab=0.$$

如果 $b=0$，则 $a^2=-1$，这是不可能的，所以必有 $a=0$，$b^2=1$，$b=\pm 1$。

（1）如果 $b=1$，则 $\sigma(i)=i$，从而

$$\sigma(x+yi)=\sigma(x)+\sigma(y)\sigma(i)=x+yi,$$

这时 σ 是恒等变换.

（2）如果 $b=-1$，则 $\sigma(i)=-i$，从而

$$\sigma(x+yi)=\sigma(x)+\sigma(y)\sigma(i)=x-yi,$$

这时，σ 是 $\mathbf{Z}[i]$的自同构.

事实上，σ 显然是一一变换，且有

$$\begin{aligned}&\sigma((x+yi)+(x_1+y_1i))\\&=b((x+x_1)+(y+y_1)i)\\&=(x+x_1)-(y+y_1)i\\&=(x-yi)+(x_1-y_1i)\\&=\sigma(x+yi)+\sigma(x_1+y_1i).\end{aligned}$$

$$\begin{aligned}&\sigma((x+yi)(x_1+y_1i))\\&=\sigma((xx_1-yy_1)+(xy_1+yx_1)i)\\&=(xx_1-yy_1)-(xy_1+yx_1)i\\&=(x-yi)(x_1-y_1i)\\&=\sigma(x+yi)\sigma(x_1+y_1i).\end{aligned}$$

总之，$\mathbf{Z}[i]$只有上述两个自同构。

六、环扩张定理

如果环R同构于环$\bar{R}$，$\bar{R}_1$是$\bar{R}$的子环，则显然R中存在子环R_1与$\bar{R}_1$同构。现在考虑问题的反面，即下面的"环扩张定理"。

定理 7 设环$\bar{R}_1 \cong R_1$，$R_1 \cap \bar{R} = \phi$，$\bar{R}_1$是环$\bar{R}$的子环，则存在R_1的扩环R，$\bar{R} \cong R$。

证明：设$R = R_1 \cup (\bar{R} \setminus \bar{R}_1)$。假定$\bar{R}_1$到$R_1$的同构映射为$\varphi$。构造$\bar{R}$到$R$的映射$\psi$如下（如图 4—2）：

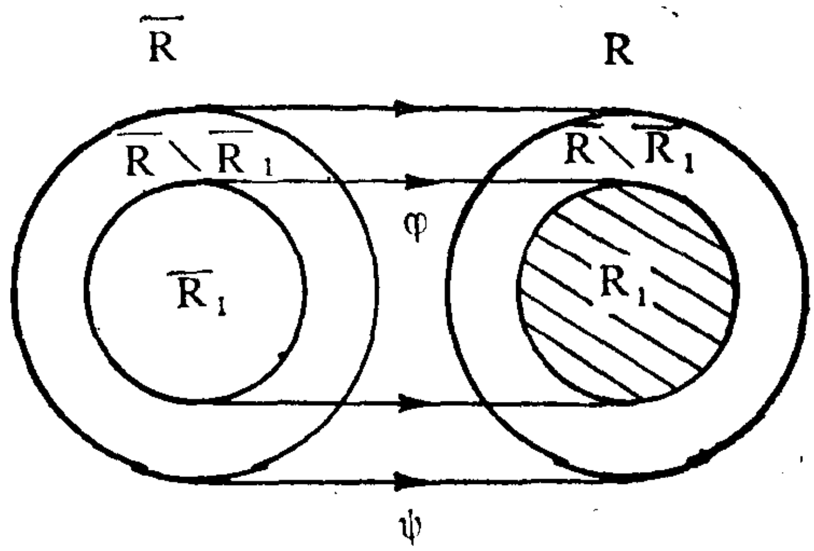


图 4—2

$$\psi(\bar{r}) = \begin{cases} \varphi(\bar{r}), & \text{当 } \bar{r} \in \bar{R}_1 \text{ 时；} \\ \bar{r}, & \text{当 } \bar{r} \in \bar{R} \setminus \bar{R}_1 \text{ 时。} \end{cases}$$

ψ是满射。事实上，R的元素如果属于R_1，则φ下的原象即ψ下的原象，如果属于$\bar{R} \setminus \bar{R}_1$，则$\psi$下的原象即元素本身。

ψ是单射。事实上，如果$\bar{r}_1 \neq \bar{r}_2$，当它们同属$\bar{R}_1$或$\bar{R} \setminus \bar{R}_1$时，显然$\psi(\bar{r}_1) \neq \psi(\bar{r}_2)$；当$\bar{r}_1 \in \bar{R}_1$，$\bar{r}_2 \in \bar{R} \setminus \bar{R}_1$时，

$\psi(\bar{r}_1)=\varphi(\bar{r}_1)\in R_1$， $\psi(\bar{r}_2)=\bar{r}_2\in\bar{R}$， 由于$R_1\cap\bar{R}=\phi$， 故 $\psi(\bar{r}_1)\neq\psi(\bar{r}_2)$。

在R中规定代数运算如下：

$$r_1\oplus r_2=\psi(\psi^{-1}(r_1)+\psi^{-1}(r_2))，$$
$$r_1\odot r_2=\psi(\psi^{-1}(r_1)\cdot\psi^{-1}(r_2))，$$

即R中两元素的和或积为$\bar{R}$中对应元素和或积的象。由于ψ是一一映射，所以$\oplus$和$\odot$是R的代数运算。任取$\bar{r}_1,\bar{r}_2\in\bar{R}$，设$\psi(\bar{r}_1)=r_1$，$\psi(\bar{r}_2)=r_2$，

$$\psi(\bar{r}_1+\bar{r}_2)=\psi(\psi^{-1}(r_1)+\psi^{-1}(r_2))=r_1\oplus r_2=\psi(\bar{r}_1)\oplus\psi(\bar{r}_2)，$$
$$\psi(\bar{r}_1\cdot\bar{r}_2)=\psi(\psi^{-1}(r_1)\cdot\psi^{-1}(r_2))=r_1\odot r_2=\psi(\bar{r}_1)\odot\psi(\bar{r}_2)。$$

所以$\langle\bar{R},+,\cdot\rangle$与$\langle R,\oplus,\odot\rangle$同构，因而后者是环，其同构映射是$\psi$。

R_1中的代数运算与R中一致。事实上，任取r_1，$r_2\in R_1$，设$r_1+r_2=r_3,\varphi^{-1}(r_1)=\bar{r}_1,\varphi^{-1}(r_2)=\bar{r}_2,\varphi^{-1}(r_3)=\bar{r}_3$。$\varphi^{-1}$是$R_1$到$\bar{R}_1$的同构，故$\bar{r}_1+\bar{r}_2=\bar{r}_3$，而在$R_1$上$\varphi^{-1}$与$\psi^{-1}$相同，故

$$\begin{aligned}r_1+r_2=r_3&=\psi(\bar{r}_3)\\&=\psi(\bar{r}_1+\bar{r}_2)\\&=\psi(\psi^{-1}(r_1)+\psi^{-1}(r_2))\\&=r_1\oplus r_2.\end{aligned}$$

同理$r_1\cdot r_2=r_1\oplus r_2$。这就证明了$R_1$是$R$的子环。

证毕

环扩张定理在证明某些环的存在性上常用到。由图可见，R是把$\bar{R}$中$\bar{R}_1$挖出，补上R_1得到的，所以此定理有人也称为“挖补定理”。

习　题　4·4

1. 设R是环，代数系$\bar{R}$有代数运算＋和·，R到$\bar{R}$的满射φ是$\langle R,+\rangle$到$\langle \bar{R},+\rangle$以及$\langle R,\cdot\rangle$到$\langle \bar{R},\cdot\rangle$的同态。求证：$\langle \bar{R},+,\cdot\rangle$是环，且$R$与$\bar{R}$环同态。

2. 设φ是环R到$\bar{R}$的同态，R有单位元，u是R的可逆元，求证：$\varphi(u)$是$\bar{R}$的可逆元的充要条件为$u\in K_{\varphi}$。

3. 设环R_1与R_2同态，R_2与R_3同态，求证：R_1与R_3同态。

4. 找出$\mathbf{Z}_{15}$到$\mathbf{Z}_3$的所有环同态映射。

5. 找出$\mathbf{Z}_7$到$\mathbf{Z}_4$的所有环同态映射。

6. 证明本节定理5。

§4·5　多项式环

我们学过数域上的多项式（见本丛书《多项式代数》），现在我们在环上建立多项式。

一、基本概念

设R是有单位元的可换环，x是一个符号，它不是R的元素，称为R上的不定元，假定它与R中的任意元素可换。形如

$$f(x)=a_0+a_1x+\cdots+a_nx^n\ (a_i\in R)$$

的表达式，称为环R上的一元多项式。a_ix^i称为第i次项，a_i称为i次项系数，a_0称为零次项，$0x^i$可以省略，$1x^i$写作x^i，如果n是非零系数项中最高次数，则称$f(x)$为n次多

项式。若多项式所有系数为零，则称为零多项式，记为$0(x)$。$0(x)$认为没有次数。只有零次项的多项式称为零次多项式。

R 上的一元多项式全体组成的集合，记为 $R[x]$。

$R[x]$中两个多项式当且仅当对应系数相等时，规定为相等。

$R[x]$中引入加法与乘法如下：

设 $f(x)=\sum_{i=0}^{n} a_i x^i$，$g(x)=\sum_{i=0}^{m} b_i x^i$，$n \geqslant m$。

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i,$$

$$f(x)g(x)=\sum_{k=0}^{m+n} c_k x^k,\ \text{其中}\ c_k=\sum_{i+j=k} a_i b_j.$$

这些都与数域上多项式的运算法则相同。

易见多项式加法、乘法满足交换律、结合律，乘法关于加法适合分配律。因而，$\langle R[x],+,\cdot\rangle$ 是一个可换环，称为环 R 上的一元多项式环。其零元是 $0(x)$，$f(x)$ 的负元是将其系数全部反号的多项式。$R[x]$ 的单位元就是 R 的单位元 1。

由于 $R \subset R[x]$，且 R 中元素的加法和乘法，与把它看成零次多项式和零多项式时在 $R[x]$中的相应运算完全一致，所以 R 是 $R[x]$的子环。

例 1 在 $\mathbf{Z}_4[x]$中计算：

$$([2]x^4-[3]x^2+[1])([2]x+[3])$$

解：

$$\begin{array}{rr}
 & [2]x^4-[3]x^2+[1] \\
\cdot) & [2]x^2-[3] \\
\hline
 & [0]x^6-[2]x^4+[2]x^2 \\
+) & -[2]x^4+[1]x^2-[3] \\
\hline
 & [3]x^4-[3]
\end{array}$$

注意：$[4]=[0]$，$[6]=[2]$，$[9]=[1]$.

例 2 在 $\mathbf{Z}_3[x]$中计算：

$$([2]x^2+[1]x-[2])^2.$$

解：

$$\begin{array}{rr}
 & [2]x^2+[1]x-[2] \\
\cdot) & [2]x^2+[1]x-[2] \\
\hline
 & [1]x^4+[2]x^3-[1]x^2 \qquad\qquad\qquad\qquad \\
 & [2]x^3+[1]x^2-[2]x \qquad\quad \\
+) & -[1]x^2-[2]x+[1] \\
\hline
 & [1]x^4+[1]x^3-[1]x^2-[1]x+[1]
\end{array}$$

在例 1 中积的次数低于因子的次数之和，例 2 中积的次数是因子次数之和. 这因为 $\mathbf{Z}_4$ 有零因子，而 $\mathbf{Z}_3$ 无零因子.

如果环 R 有零因子，R 的零因子也是 $R[x]$的元素，所以也是 $R[x]$的零因子. 反之，如果 R 无零因子，只要 $f(x)$ 和 $g(x)$都不是零多项式，根据乘法法则，$f(x)g(x)$ 的次数是 $f(x)$与 $g(x)$的次数之和，因而 $f(x)g(x)$也不是零多项式.这样就得到

定理 1 有单位元的可换环 R 上的多项式环 $R[x]$ 也是有单位元的可换环. $R[x]$是整环当且仅当 R 是整环.

二、多元多项式环

设 R 是有单位元的可换环，x_1 是 R 的不定元，那末 $R[x_1]$ 又是一个有单位元的可换环. 其单位元即 R 的单位元 1. 现在在 $R[x_1]$上再添加新的不定元 x_2，得到 $R[x_1][x_2]$，同样可以继续添加有限个不定元，得到 $R[x_1][x_2]\cdots[x_n]$，假定这些不定元不仅可以与 R 的元素交换，也可以互相交换. $R[x_1][x_2]\cdots[x_n]$的元素可以写成以下形式：

$$f(x_1,\cdots,x_n)=ax_1^{k_1}\cdots x_n^{k_n}+\cdots+bx_1^{j_1}\cdots x_n^{j_n}.$$

（$a,\cdots,b$ 是R的元素）

这样形成的多项式环仍是一个有单位元的可换环，称为R上的n元多项式环，记为$R[x_1,\cdots,x_n]$。如果R是整环，则$R[x_1,\cdots,x_n]$也是整环。

三、多项式的根

设S是有单位元的可换环，R是S的子环，且含有R的单位元。再设$C\in S$，

$$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x],$$

规定

$$f(c)=a_0+a_1c+\cdots+a_nc^n(\in S).$$

如果$f(c)=0$，则称c是$f(x)$的根。

固定c，每个$f(x)$决定一个元素$f(c)$，当$f(x)$跑遍$R[x]$时，$f(c)$构成S的子集合，记为$R[c]$。

定理 2 设S是有单位元的可换环，$c\in S$，R是S的子环，$1\in R$，则$R[c]$是S的子环。

证明：规定$R[x]$到S的映射如下：

$$\sigma(f(x))=f(c).$$

σ是同态映射。事实上，设

$$f(x)+g(x)=h(x),\quad f(x)g(x)=k(x),$$

那末，

$$\sigma(h(x))=h(c)=f(c)+g(c)=\sigma(f(x))+\sigma(g(x));$$

$$\sigma(k(x))=k(c)=f(c)g(c)=\sigma(f(x)g(x)).$$

因而σ的象集$\sigma[R[x]]=R[c]$是S的子环。

证毕

$R[c]$既然是子环，就一定包含S的零元，即存在R上的多项式，以c为根。这样的多项式如果只有$0(x)$，就是说，c不是R上任意非零多项式的根，则称c是环R的超越元。反之，如果存在R上的非零多项式，以c为根，则称c为环R的代数元。

R的元素都是R的代数元，因为R中元素r是多项式$x-r$的根。

i是$\mathbf{Q}$的代数元，因为它是多项式x^2+1的根。$\pi=3.1415\cdots$和$e=2.718\cdots$都是$\mathbf{Q}$的超越元（π和e的超越性，证明很繁，这里从略）。

例 3　$c=\sqrt{2}+\sqrt{6}$是不是$\mathbf{Z}$的代数元？

解：

$$c^2=2+6+4\sqrt{3}=8+4\sqrt{3},$$

$$(c^2-8)^2=(4\sqrt{3})^2=48,$$

即

$$c^4-16c^2+16=0.$$

所以，$\sqrt{2}+\sqrt{6}$是$f(x)=x^4-16x^2+16\in\mathbf{Z}[x]$的根，即是$\mathbf{Z}$的代数元。

如果c是R的代数元，由$f(c)=g(c)$不能推出$f(x)=g(x)$。因设c是非零多项式$h(x)$的根，那末

$$f(x)+h(x)\neq f(x),$$

但

$$f(c)+h(c)=f(c)+0=f(c).$$

而超越元就不同了，我们有

定理 3　如果c是环R的超越元，$f(x)$，$g(x)\in R[x]$，由$f(c)=g(c)$可以推出$f(x)=g(x)$。

证明： 如果$f(x)\neq g(x)$，则$f(x)-g(x)\neq 0(x)$，但$f(c)-g(c)=0$，所以c是非零多项式$f(x)-g(x)$的根，c是代数元，矛盾。

证毕

四、带余除法

定理 4 设R是有单位元的可换环，

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in R[x],$$

$$g(x)=b_mx^m+b_{m-1}x^{m-1}+\cdots+b_0\in R[x],$$

$a_n\neq 0$，b_m是R的可逆元，则存在R上的唯一的多项式$q(x)$和$r(x)$，使

$$f(x)=q(x)g(x)+r(x), \tag{1}$$

其中$r(x)$为$0(x)$或次数低于m。

证明：存在性。

如$n<m$，可取$q(x)=0(x)$，$r(x)=f(x)$，则（1）式成立。

下面假定$n\geqslant m$。设

$$f_1(x)=f(x)-(a_nb_m^{-1}x^{n-m})g(x),$$

其中x^n的系数是$a_n-(a_nb_m^{-1})b_m=0$。因而$f_1(x)$至多是$n-1$次多项式。如果f_1是零多项式，或次数低于m，则可取$q(x)=a_nb_m^{-1}x^{n-m}$，b_m^{-1}是可逆元，故不是零因子，所以$q(x)\neq 0(x)$，再令$r(x)=f_1(x)$，则(1)式成立。

如果f_1的次数$k\geqslant m$，设x^k的系数是$c\neq 0$，令

$$\begin{aligned}f_2(x)&=f_1(x)-cb_m^{-1}x^{k-m}g(x)\\&=f(x)-(a_nb_m^{-1}x^{n-m}+cb_m^{-1}x^{k-m})g(x).\end{aligned}$$

如果f_2的次数$<m$，或$f_2(x)=0(x)$，则可取

$$q(x)=a_nb_m^{-1}x^{n-m}+cb_m^{-1}x^{k-m},$$

$$r(x)=f_2(x),$$

否则，继续进行上述过程，由于$g(x)$的次数一定，经有限次

步骤，必然得适合上述条件的 $q(x)$ 和 $r(x)$。

唯一性。

设又有 $q_1(x)$ 和 $r_1(x)$ 满足条件，则

$$[q(x)-q_1(x)]g(x)=r_1(x)-r(x). \quad (2)$$

如果 $r_1(x)-r(x)\neq 0(x)$，设次数为 l_1，则 $l_1<m$，$q(x)-q_1(x)\neq 0(x)$，且其次数 $l_2\geqslant 0$。由于 b_m 可逆，故不是零因子，(2)式左端次数是 $m+l_2$，出现矛盾，因而 $r_1(x)-r(x)=0(x)$，$r_1(x)=r(x)$。b_m 不是零因子，如 $q(x)-q_1(x)\neq 0(x)$，则 (2) 式左端不等于 $0(x)$。所以 $q(x)-q_1(x)=0(x)$，$q(x)=q_1(x)$。

证毕

定理 4 中的 $q(x)$ 和 $r(x)$ 分别称为 $g(x)$ 除 $f(x)$ 的商式和余式。

例 3 在 $\mathbf{Z}_3[x]$ 中，已知

$$f(x)=[2]x^4+[1]x^3-[1]x^2-[1],$$

$$g(x)=[1]x^2-[1]x+[2],$$

求 $g(x)$ 除 $f(x)$ 的商式和余式。

解：

$$\begin{array}{r|l}
 & [2]x^2 \qquad\qquad -[2] \\
\hline
[1]x^2-[1]x+[2] & [2]x^4+[1]x^3-[1]x^2-[1] \\
 & [2]x^4-[2]x^3+[1]x^2 \\
\hline
 & \qquad\qquad -[2]x^2-[1] \\
 & \qquad\qquad -[2]x^2+[2]x-[1] \\
\hline
 & \qquad\qquad\qquad\qquad -[2]x
\end{array}$$

所以商式为 $[2]x^2-[2]=[2]x^2+[1]$，余式为 $-[2]x=[1]x$。

定理 5（余式定理） 设 R 是有单位元的可换环，$f(x)\in R[x]$，$a\in R$，则 $x-a$ 除 $f(x)$ 的余式为 $f(a)$。

证明：由定理4，存在多项式$q(x)$满足$f(x)=q(x)(x-a)+r(x)$，$r(x)$是$0(x)$或零次多项式，记为r，则$f(x)=q(x)(x-a)+r$，从而$f(a)=q(a)(a-a)+r$，$r=f(a)$。

证毕

在半群$\langle R[x],\cdot\rangle$中，显然$g(x)|f(x)$当且仅当$g(x)$除$f(x)$的余式为$0(x)$。

由定理5直接可得

定理6（因式定理）设R是有单位元的可换环，$a\in R$，则$x-a|f(x)$当且仅当$f(a)=0$。

习题 4·5

1．在$\mathbf{Z}_5[x]$中计算：

（1）$([2]x^2+[2]x-[3])([2]x^2+[4]x-[3])$；

（2）$([2]x+[3])^3$。

2．下列元素哪些是$\mathbf{Z}$的代数元？若是，试写出以其为根的次数最低的多项式。

（1）$\frac{3}{4}$；　　（2）$\sqrt{2}$；

（3）$\sqrt{3}+\sqrt{5}$；　　（4）$2-\pi$。

3．已知$\mathbf{Z}_4[x]$中$f(x)=[2]x^3-[1]x+[2]$，$g(x)=[1]x^2+[2]x-[2]$。求$g(x)$除$f(x)$的商式和余式。

4．找出$[1]x^5+[3]x^3+[1]x^2+[2]x\in\mathbf{Z}_5[x]$的所有根。

5．分解因式：

$$[1]x^4+[3]x^3+[2]x+[4]\in\mathbf{Z}_5[x].$$

6．设R是有单位元的可换环，$R[x]$到R的映射为$\sigma(f(x))=f(0)$，求证σ是同态。写出σ的同态核。

7. 设R为整环，问$R[x]$的可逆元有哪些？

8. 在$\mathbf{Z}_5[x]$中，设$I=\langle[2]x+[3]\rangle$，求商环$\mathbf{Z}_5[x]/I$中$([3]x^2-[1]x+[1])+I$与$([2]x-[1])+I$的积.

9. 求证：整环R上的n次多项式至多在R中有n个根.

§4·6 唯一分解环

我们在第二章学过唯一分解半群. 任意非零环R的乘半群$\langle R,\cdot\rangle$不可能是唯一分解半群(因为有零元). 当R是整环时，R^*成为R的可换可消子半群，R^*如果作成唯一分解半群，则R的每个非零不可逆元都可以分解为既约元的乘积，且任意两个分解相伴. 这一节，除介绍唯一分解环的概念外，还讲两种特殊的唯一分解环，即主理想环和欧氏环.

一、唯一分解环

定义1 设R是整环，如果$\langle R^*,\cdot\rangle$是唯一分解半群，则称R为唯一分解环.

整环的元素分为四类：零元、可逆元、既约元、可约元. 每个可约元不一定能唯一（不计相伴的差别）地分解为有限个既约元的乘积，但是唯一分解环却能做到这一点.[注]

例1 整数环$\mathbf{Z}$和实多项式环$\mathbf{R}[x]$是唯一分解环，因为$\langle \mathbf{Z}^*,\cdot\rangle$和$\langle \mathbf{R}^*[x],\cdot\rangle$都是唯一分解半群(见§2·3)

例2 任意域都是唯一分解环，因为域的非零元是可逆元.

注 对于具体的整环，这四类中可能有空集.

例 3 设 $R=\{a+b\sqrt{5}\,i\mid a,b\in\mathbf{Z}\}$。$R$ 关于数的加法与乘法作成环，且是整环。$\langle R^*,\cdot\rangle$ 不是唯一分解半群（见§2·3 例 3），所以 R 不是唯一分解环。

有一类唯一分解环是常见的，这就是主理想环。

二、主理想环

整环的每个元素 a，都可以生成一个主理想 $\langle a\rangle$。主理想是一种特殊的理想，但不一定能概括所有的理想。那末，有没有这样的整环，其所有理想都是主理想？

定义 2 如果整环 R 的所有理想都是主理想，则称 R 为主理想环。

例 4 整数环 $\mathbf{Z}$ 是主理想环。

证明： $\mathbf{Z}$ 是整环。设 I 是 $\mathbf{Z}$ 的理想。如果 $I=\{0\}$，则 $I=\langle 0\rangle$，是主理想。现在设 $I\neq\{0\}$，在 I 中取最小的正整数，设为 a。任取 $b\in I$，用 a 除 b，可得商 q 和余数 r：

$$b=qa+r.$$

其中 $0\leqslant r<a$。由于 $a\in I$，$q\in\mathbf{Z}$，故 $qa\in I$，又 $b\in I$，所以 $r=b-qa\in I$。由 a 的最小性，推得 $r=0$。即 $b=qa\in\langle a\rangle$，$I\subseteq\langle a\rangle$。

反之，由于 $a\in I$，故 $\langle a\rangle\subseteq I$。

总之，$I=\langle a\rangle$。

例 5 整数环上的多项式环 $\mathbf{Z}[x]$ 不是主理想环。

分析： 找出 $\mathbf{Z}[x]$ 的一个理想，然后证明它不是主理想。

证明： 设 $E=\langle x,2\rangle$，$E=\langle x\rangle+\langle 2\rangle$。$\langle x\rangle$ 是一切常数项为零的多项式集合，$\langle 2\rangle$ 是一切偶系数多项式的集合．因而 E

是由所有常数项为偶数的多项式组成。

若 $E=\langle f(x)\rangle$，由于 $2\in E$，所以存在 $g(x)\in \mathbf{Z}[x]$，使 $2=f(x)g(x)$。因而 $f(x)$为零次多项式，即是一个非零偶数，它只能是 ± 2，$g(x)$只能是 ± 1。由于 $x\in E$，故存在 $h(x)\in \mathbf{Z}[x]$，使

$$x=f(x)h(x)=\pm 2h(x),$$

$$h(x)=\pm\frac{x}{2}\bar{\in}\mathbf{Z}(x).$$

出现矛盾。所以 E 不是主理想，$\mathbf{Z}[x]$不是主理想环。

三、主理想环中的因子分解

主理想环是唯一分解环，这是主理想环最重要的性质。为了证明这一点，我们分成几步来作。

定理 1 主理想环 R 中所有非零不可逆元都能分解为既约元的乘积。[注]

证明： 用反证法。设 a 是 R 的非零不可逆元，a 不能分解为既约元的乘积（既约元本身认为已经分解为既约元的乘积）。自然，a 不是既约元，因而存在 a 的真因子 b 和 c，使 $a=bc$。b 和 c 中至少有一个不能分解为既约元的乘积，因为否则 a 也就分解为既约元的乘积了。设这个元素是 b，令 $a_1=b$。同样又可得到 a_1 的真因子 a_2，它不能分解为既约元的乘积。于是，得到无限元素列：

$$a,\ a_1,\ a_2,\ \cdots.$$

其中每个元素是前一个元素的真因子。这样，得到一系列主理想的包含关系：

注 “分解为既约元的乘积”是指分解为有限个既约元的乘积。

$$\langle a\rangle\subseteq\langle a_1\rangle\subseteq\langle a_2\rangle\subseteq\cdots.$$

取 $I=\langle a\rangle\cup\langle a_1\rangle\cup\langle a_2\rangle\cup\cdots$. 我们来证明 I 是理想。

事实上，任取 i_1, $i_2\in I$, 不妨设 $i_1\in\langle a_n\rangle$, $i_2\in\langle a_m\rangle$, $n\leqslant m$, 则 $i_1-i_2\in\langle a_m\rangle\subseteq I$. 任取 $i\in I$, $r\in R$, 设 $i\in\langle a_k\rangle$, 则 $ri=ir\in\langle a_k\rangle\subseteq I$. 所以 I 是理想。

由于 R 是主理想环，I 是主理想，故存在非零元 d, 使 $I=\langle d\rangle$. 这时，

$$a, a_1, a_2, \cdots\in\langle d\rangle.$$

d 是上述 a_i 的公共因子。既然 $d\in I=\bigcup_{i=1}^{\infty}\langle a_i\rangle\cup\langle a\rangle$, d 必属于某个 $\langle a_m\rangle$. 所以 a_m 是 d 的因子。因而也是所有 a, a_1, $a_2, \cdots$ 的公共因子，自然是 a_{m+1} 的因子，但 a_{m+1} 是 a_m 的因子，所以 a_m 与 a_{m+1} 相伴，a_{m+1} 不是 a_m 的真因子，出现矛盾。

证毕

为了证明分解的唯一性，须先介绍最大公因子的概念。它实际上是半群中的概念，不过这里在整环中引出。

定义 3 设 R 是一个整环，$a, b\in R$, 如果 $c\in R$ 是 a 与 b 的公共因子，则称 c 为 a 与 b 的公因子。如果 d 是 a 与 b 的公因子，且 a 与 b 的所有公因子都是 d 的因子，则称 d 是 a 与 b 的最大公因子。全体最大公因子的集合记为 (a,b).

公因子和最大公因子的概念可以推广到多个元素的情况。

在整环中，单位元以至可逆元都是任意元素的因子，因而是任意一组元素的公因子。如果 d 是 a, b 的最大公因子，那末与 d 相伴的元素也是 a, b 的最大公因子。所以最大公因子实际上是一个相伴类，因而论及最大公因子时，不计较相伴的差别。一般的整环不一定任意两个元素都有最大公因

子，但我们有

定理 2 主理想环R中任意两个元素总有最大公因子。

证明：设a，b是R的任意元素。由a，b生成的理想是$\langle a\rangle+\langle b\rangle=\{ar+bs \mid r,s\in R\}$。它是主理想，设$\langle a\rangle+\langle b\rangle=\langle d\rangle$，则

$$a=a\cdot 1+b\cdot 0\in\langle d\rangle,\ b=a\cdot 0+b\cdot 1\in\langle d\rangle.$$

因而d是a，b的公因子。

如果c是a，b的公因子，则$a\in\langle c\rangle$，$b\in\langle c\rangle$，从而一切形如$ar+bs$的元素也属于$\langle c\rangle$。即$\langle d\rangle\subseteq\langle c\rangle$，因而$d\in\langle c\rangle$，$c$是$d$的因子。

总之，$d\in(a,b)$。

证毕

引理 1 在主理想环中，

$$(ac,bc)=(a,b)c. \tag{1}$$

注意：(1)式是两个子集相等。

证明：先假定$c\neq 0$且a,b不全为零。任取$d\in(a,b)$，则$dc|ac$，$dc|bc$，dc整除ac与bc的最大公因子集(ac,bc)的任一元素d_1。设$d_1=dcq$，$ac=d_1k$，则$ac=dcqk$，消去c，得$a=dqk$。同样可得$b=dql$。于是，dq是a与b的公因子，故$dq|d$。由于a，b不全为零，故$d\neq 0$，所以q必为可逆元，$dc|d_1$。即d_1与dc相伴，推得(1)式。

如果$c=0$或$a=b=0$，由于$(0,0)=\{0\}$，所以(1)仍成立。

证毕

引理 2 在主理想环中

$$((a,b),c)=(a,(b,c)). \tag{2}$$

证明： 任取 $d_1 \in (a,b)$，$d_2 \in (b,c)$，$d_3 \in (d_1,c)$，则 $d_3 | d_1$，$d_3 | c$，因而 $d_3 | a, d_3 | b$，$d_3 | c$，于是 $d_3 | d_2$. d_3 整除 a 和 d_2 的任一最大公因子 d_4。反之，同样可证 a 和 d_2 的任一最大公因子 d_4 必然也整除 d_1 与 c 的任一最大公因子 d_3。所以 d_3 与 d_4 相伴，(2)式成立。

证毕

定义 4 整环中元素 a，b 如果公因子只有可逆元，则称 a 与 b 互素。

引理 3 在主理想环中，如果 a 与 b 互素，a 与 c 互素，则 a 与 bc 互素。

证明： 设 k 是 a 与 bc 的任一公因子，只须证明 k 是可逆元。由于 $1 \in (a,b)$，据引理 1，$c = 1c \in (ac, bc)$。而 k 是 ac 与 bc 的公因子，故 $k | c$，所以 k 是 a 与 c 的公因子。a 与 c 互素，故 k 是可逆元。

证毕

引理 4 设 p 是主理想环 R 的既约元，如果 $p | ab$，则或者 $p | a$，或者 $p | b$ 至少有一成立。

证明： 用反证法。假如 $p \nmid a$，$p \nmid b$，a 和 p 的公因子是 p 的因子，所以只能是可逆元或 p 的相伴元。若是 p 的相伴元，那末 $p | a$，所以 a 和 p 的公因子只有可逆元，即 a 与 p 互素。同理 b 与 p 互素。由引理 3，ab 与 p 互素。因 $p | ab$，故 $p | 1$，p 必为可逆元，矛盾。说明或者 $p | a$，或者 $p | b$ 至少有一成立。

证毕

有了上面的准备，我们可以证明主理想环的唯一分解性质了。

定理 3 主理想环 R 中任意非零不可逆元分解为既约元

乘积时，除了相伴的差别外，是唯一的。

证明：设 a 是 R 的非零不可逆元。由定理 1，a 分解为既约元的乘积：

$$a = p_1 p_2 \cdots p_m.$$

对 m 实行归纳法。当 $m=1$ 时，a 为既约元，因而分解是唯一的。现在假定定理对 $m-1$ 成立。让我们对 m 的情况推证定理成立。

设 a 又分解为既约元 q_i 的乘积：

$$a = q_1 q_2 \cdots q_n.$$

于是，得到等式

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n. \tag{2}$$

$p_1 | q_1 q_2 \cdots q_n$，由引理 4，q_1，q_2，…，q_n 中至少有一个被 p 整除，设为 q_1。q_1 也是既约元，因而 p_1 与 q_1 相伴。设 $q_1 = p_1 \varepsilon$，代入(2)，得

$$p_1 p_2 \cdots p_m = p_1 \varepsilon q_2 \cdots q_n.$$

消去 p_1，于是又有

$$p_2 \cdots p_m = \varepsilon q_2 \cdots q_n. \tag{3}$$

(3)式两端是 a 的真因子的既约元分解式。左端因子有 $m-1$ 个，由归纳假定，$m-1=n-1$，且对应因子相伴。又由 q_1 和 p_1 相伴，所以 a 的以上两种分解是相伴的分解。

证毕

综合定理 1 和定理 3，得到

定理 4 主理想环是唯一分解环。

三、欧氏环

下面介绍一类更特殊的环，它是主理想环中重要的一

类。

我们知道，在实多项式环中，每个非零多项式都有次数，它是一个非负整数。在整数环中，每个非零整数也对应一个非负整数，即绝对值。这两种非负整数在两个环的欧氏除法（即带余除法）中起着类似的作用。以上两个环的直接推广，就是欧氏环。

定义 5 设R是整环。如果存在定义在R^*上的非负整数值的函数σ（即R^*到$\mathbf{N}$的映射），满足以下条件：对于任意的a，$b\in R$，$a\neq 0$，R中存在适合等式

$$b=qa+r \tag{4}$$

的元素q，r，而$r=0$或$\sigma(r)<\sigma(a)$。这时，称R为欧几里德(Euclid)环注，或欧氏环。

例 6 整数环是欧氏环，其中$\sigma(a)=|a|$。

例 7 设F是域，F上的多项式环$F[x]$是欧氏环。事实上，取$\sigma(f(x))=f(x)$的次数，则由§4·5 定理 4，对于任意多项式$f(x)$和$g(x)\neq 0(x)$存在$q(x)$和$r(x)$，使$f(x)=q(x)g(x)+r(x)$。其中$r(x)=0(x)$，或次数低于$g(x)$的次数，即$\sigma(r(x))<\sigma(g(x))$。

例 8 任意域是欧氏环。

事实上，恒取$\sigma(a)=0(a\neq 0)$。设$a\neq 0$，则a可逆，对于任意的b，有$b=(ba^{-1})a+0$。这时，$q=ba^{-1}$，$r=0$。

定理 5 欧氏环是主理想环。

证明：设I是欧氏环R的任一理想。如果I是零理想，则I显然是主理想。下面设$I\neq\{0\}$，I的非零元集为I^*，则

注 Euclid是公元前三世纪希腊著名数学家，著有《原本》。欧氏环的命名是因为可以在该环中施行"欧几里德除法"。

$I^*\neq\phi$. $\sigma[I^*]$ 是非负整数的集合，其中必有最小者，设为 $\sigma(a)(a\in I^*)$。对于任意的 $b\in I$，存在 q，$r\in R$，使 $b=qa+r$。这时，如果 $r\neq 0$，由欧氏环的性质，$\sigma(r)<\sigma(a)$，而 $r=b-qa\in I$，与 a 的选择矛盾。因此 $r=0$，即 $b=qa$，$I=\langle a\rangle$是主理想。

R 的任意理想是主理想，所以 R 是主理想环。

证毕

推论 1 欧氏环是唯一分解环。

这样一来，我们看到，欧氏环是主理想环，主理想环是唯一分解环。反之，唯一分解环不一定是主理想环，主理想环也不一定是欧氏环。

在例 7 中，我们看到，域 F 的多项式环 $F[x]$是欧氏环。因而有

定理 6 域 F 的多项式环 $F[x]$是主理想环。

注意：整环 R 上的多项式环 $R[x]$不一定是主理想环，见例 5。

域 F 上的多项式环 $F[x]$的既约元，常称为既约多项式，或不可约多项式。如 x^2+x+1，$x+1$，都是实数域上的既约多项式；x^2-2 是有理数域上的既约多项式，但不是实数域上的既约多项式，因为 $x^2-2=(x+\sqrt{2})(x-\sqrt{2})$。

例 9 求证：$f(x)=[1]x^3+[1]x^2+[2]$是 $\mathbf{Z}_3[x]$中的既约多项式。

证明：若不然，$f(x)$有真因式，其真因式只能是一次或二次多项式，因而 $f(x)$ 在 $\mathbf{Z}_3$ 中有根，但易见 $f([0])=[2]$，$f([1])=[1]$，$f([2])=[2]$。说明 $f(x)$ 无根，因而 $f(x)$是既约多项式。

例10　在$\mathbf{Z}_5[x]$中分解多项式$[1]x^4+[1]$为既约多项式的乘积。

解：易见 $[1]x^4+[1]=([1]x^2+[2])([1]x^2+[3])$。而上式右端两个因式是既约多项式，因为否则它们必有一次因子，即在$\mathbf{Z}_5$中有根。但可以验证，$\mathbf{Z}_5$的所有元素都不是它们的根。

唯一分解环R上的多项式环一般不是主理想环，但可以证明$R[x]$，以至多元多项式环$R[x_1,\cdots,x_n]$，也是唯一分解环。

习　题　4·6

1. 下列元素哪些是对应整环的既约元？

(1) $5\in\mathbf{Z}$;　　(2) $-17\in\mathbf{Z}$;

(3) $14\in\mathbf{Z}$;　　(4) $2x-3\in\mathbf{Z}[x]$;

(5) $2x-10\in\mathbf{Z}[x]$;　　(6) $2x-10\in\mathbf{Q}[x]$;

(7) $[2]x-[5]\in\mathbf{Z}_7[x]$;

(8) $[1]x^2-[3]x+[2]\in\mathbf{Z}_5[x]$。

2. 将$4x^2-4x+8$在$\mathbf{Z}[x]$中分解为既约多项式之积。

3. 设在整环中，d是a，b的最大公因子，$a=da_1$，$b=db_1$，求证：a_1与b_1互素。

4. 在高斯数环$\mathbf{Z}[i]$中，设$N(a+bi)=a^2+b^2$，求证：对于任意α，$\beta\in\mathbf{Z}[i]$，有

(1) $N(\alpha)\geqslant 0$;

(2) $N(\alpha)=0\Longleftrightarrow\alpha=0$;

(3) $N(\alpha\beta)=N(\alpha)N(\beta)$;

(4) $\mathbf{Z}[i]$的可逆元由$1,-1,i,-i$组成；

(5) 若 $N(a)=p$ 是素数，则 a 是既约元.

5. 设 R 是整环，但不是域，求证 $R[x]$ 不是主理想环.

6. $7+0i$ 是否 $\mathbf{Z}[i]$ 的既约元?

7. 分解多项式 $[1]x^3+[2]x^2+[2]x+[4]\in\mathbf{Z}_7[x]$ 为既约多项式之积.

8. 设 R 是主理想环，d 是 a 与 b 的最大公因子，求证：存在 $u,v\in R$，使 $au+bv=d$. 由此证明 a,b 互素的充要条件是存在 $u,v\in R$，使 $au+bv=1$.

9. 设 R 是主理想环，R_1 是 R 的子环且是主理想环，求证：a 与 b 若在 R_1 中互素必然也在 R 中互素.

§4·7 素理想与最大理想

一个环至少有平凡理想. 此外，还可能有真理想. 每个理想生成一个商环，如果商环具有一些特定的性质，如是整环、是域等，反过来，对理想就有相应的要求，从而产生出一些特殊的理想. 这节讨论两种特殊的理想，即素理想与最大理想.

一、素理想

如果 p 是素数，$p|ab$，那末 p 必整除 a 或 b. 如果 p 不是素数，就没有这一性质. 一个整数 a 整除整数 b，也可以表示成：$b\in\langle a\rangle$.

素数的上述性质可以表为理想的性质：

如果 $ab\in\langle p\rangle$，则或者 $a\in\langle p\rangle$，或者 $b\in\langle p\rangle$.

定义 1 设 P 是可换环 R 的理想，它具有下述性质：如

果 $ab\in P$，则 $a\in P$ 或 $b\in P$. 这时，称 P 为 R 的素理想。

单位理想显然是素理想. 零理想 $\langle 0\rangle$ 不一定是素理想. 如当 R 有零因子时，存在 $a\neq 0$，$b\neq 0$ 却有 $ab=0$，即 $ab\in\langle 0\rangle$，$a\notin\langle 0\rangle$，$b\notin\langle 0\rangle$。而当 R 无零因子时，显然零理想是素理想。

素理想生成的商环是什么样的呢？

定理 1 可换环 R 中，理想 P 是素理想的充要条件是商环 R/P 无零因子。

证明：设 P 是 R 的素理想. 任取 R/P 的两个非零元 $a+P$ 和 $b+P$，如果 $(a+P)(b+P)=P$（P 是 R/P 的零元），那末 $ab+P=P$，$ab\in P$. 因而 $a\in P$ 或 $b\in P$，即 $a+P=P$ 或 $b+P=P$，说明 R/P 无零因子。

反之，如果 R/P 无零因子. 设 $ab\in P$，即

$$ab+P=P,\quad (a+P)(b+P)=P.$$

因而，$a+P=P$，或 $b+P=P$，即 $a\in P$ 或 $b\in P$. P 是素理想。

证毕

推论 1 如果 R 是有单位元的可换环，理想 P 是素理想的充要条件是商环 R/P 是整环。

证明：只须注意由于 R 有单位元，则 R 的商环也有单位元。由定理得证。

例 1 求证：$\langle x\rangle$ 和 $\langle 2,x\rangle$ 是 $\mathbf{Z}[x]$ 的素理想。

证明：作 $\mathbf{Z}[x]$ 到 $\mathbf{Z}$ 的映射 φ 如下：

$$\varphi(a_0+a_1x+\cdots+a_nx^n)=a_0.$$

显然，φ 是满同态. 其同态核为

$$\langle x\rangle=\{a_1x+\cdots+a_nx^n\mid n>0,\ a_1,\cdots,a_n\in\mathbf{Z}\}.$$

由环的同态基本定理，$\mathbf{Z}[x]/\langle x\rangle\cong\mathbf{Z}$. $\mathbf{Z}$ 是整环，因而$\langle x\rangle$是素理想。

作 $\mathbf{Z}[x]$到$\mathbf{Z}_2$的映射 ψ 如下：

$$\psi(a_0+a_1x+\cdots+a_nx^n)=\begin{cases}[0], & \text{当 } a_0 \text{ 是偶数},\\ [1], & \text{当 } a_0 \text{ 是奇数}.\end{cases}$$

ψ是φ及$\mathbf{Z}$到$\mathbf{Z}_2$的自然同态的合成，因而是同态，显然是满同态。其同态核为

$$\{a_0+a_1x+\cdots+a_nx^n \mid n\geqslant 0,\ a_0 \text{ 是偶数},\ a_1,\cdots,\ a_n\in\mathbf{Z}\}=\langle 2,x\rangle.$$

(参见§4·6 例 5)$\mathbf{Z}[x]/\langle 2,x\rangle\cong\mathbf{Z}_2$，$\mathbf{Z}_2$是整环，故$\langle 2,x\rangle$是素理想。

例 2　整数环的素理想有哪些？

解：$\mathbf{Z}$ 无零因子，故$\langle 0\rangle$和$\mathbf{Z}$ 都是$\mathbf{Z}$ 的素理想。$\mathbf{Z}$ 是主理想环，$\mathbf{Z}$ 的任意理想是主理想。$\mathbf{Z}/\langle n\rangle=\mathbf{Z}_n$ 无零因子当且仅当n是素数（见§4·2 例 2 ），故$\langle n\rangle$是素理想当且仅当n是素数。这里假定$n>1$.

所以，$\mathbf{Z}$ 的素理想有三类：零理想、单位理想和$\langle p\rangle$，其中p为素数。

二、最大理想

定义 2　设M是环R的理想。如果除了R和M外，没有包含M的理想，则称M是R的最大理想。

环R的单位理想R显然是最大理想。

例 3　$\mathbf{Z}$ 的最大理想有哪些？

解：除单位理想外，设M是最大理想，$M=\langle n\rangle$，$n>1$. 如果n不是素数，则$n=n_1n_2$，n_1是n的真因子。因而

$\langle n\rangle\subseteq\langle n_1\rangle$，且$\langle n\rangle\neq\langle n_1\rangle$，$\langle n_1\rangle\neq\mathbf{Z}$。于是，$\langle n\rangle$不是最大理想。

反之，设 p 是素数，$M=\langle p\rangle$，如果理想 $N\supset\langle p\rangle$，则有 $a\in N$，$a\bar{\in}\langle p\rangle$，即 $p\nmid a$。于是$(a,p)=1$，即存在 $u,v\in\mathbf{Z}$，使 $ua+vp=1$。由于 $ua\in N$，$vp\in\langle p\rangle\subset N$，因而 $1\in N$。即 $N=\mathbf{Z}$。所以除 $\mathbf{Z}$ 和$\langle p\rangle$之外，没有包含$\langle p\rangle$的理想，$\langle p\rangle$是最大理想。

所以 $\mathbf{Z}$ 的最大理想共有两类：单位理想和$\langle p\rangle$，其中 p 为素数。

上例说明，$\mathbf{Z}$ 的最大理想总是素理想。这个事实具有一定的普遍性，为了证明它，先讲一个最大理想的性质。

定理 2 有单位元的可换环 R 中，真理想 M 为最大理想的充要条件是：R/M 是域。

证明：如果 M 是最大理想，为证 R/M 是域，只须证明对于任意的 $\bar{a}$，$\bar{b}\in R/M$，$\bar{a}\neq\bar{0}$，方程 $\bar{a}\bar{x}=\bar{b}$ 总有解。(这里用 $\bar{a}$ 表示 a 所在的陪集，即 $\bar{a}=a+M$，$\bar{0}=M$)

由 a 和 M 生成的理想 $N=\langle a,M\rangle=\langle a\rangle+M$ 包含 M，且不等于 M($a\in N$，$\bar{a}\neq\bar{0}$，即 $a\bar{\in}M$)。所以 $N=R$。于是 R 中的任意元素 $b\in\langle a\rangle+M$，即可表 $b=ar+m(r\in R,\ m\in M)$，$b-ar\in M$。这样，

$$\bar{b}-\overline{ar}=\overline{b-ar}=\bar{0}.$$

$$\bar{a}\bar{r}=\overline{ar}=\bar{b}.$$

$\bar{r}$ 是方程 $\bar{a}\bar{x}=\bar{b}$ 的解。

反之，如果 R/M 是域，N 是含 M 的理想，$N\neq M$，则有 $a\in N$，$a\bar{\in}M$。$\bar{a}\neq\bar{0}$，故方程 $\bar{a}\bar{x}=\bar{b}$ 对任意 $b\in R$ 有解。设解为 $\bar{r}$，即知

$$\overline{ar}-\bar{b}=\bar{0},\quad \overline{ar-b}=\bar{0},$$

或 $$ar-b=m\in M.$$
而 $ar\in N$, $M\subseteq N$,故 $b=ar-m\in N$. b 是 R 的任意元素,推得 $R=N$. 即包含 M 的理想除 M 外只有 R, 说明 M 是最大理想.

证毕

定理 3 有单位元的可换环中,最大理想是素理想.

证明: 最大理想生成的商环是域,域无零因子,由定理 1 得证.

例 4 $\mathbf{Z}[x]$中,$\langle 2,x\rangle$是最大理想,而$\langle x\rangle$不是最大理想.

证明: $\mathbf{Z}[x]/\langle x\rangle\cong\mathbf{Z}$, 而 $\mathbf{Z}[x]/\langle 2,x\rangle\cong\mathbf{Z}_2$, $\mathbf{Z}$ 不是域而 $\mathbf{Z}_2$ 是域,故$\langle 2,x\rangle$是最大理想,$\langle x\rangle$不是最大理想,$\langle x\rangle$是素理想.

实际上,上述事实可从$\langle x\rangle\subseteq\langle 2,x\rangle\subseteq\mathbf{Z}[x]$,$\langle x\rangle\neq\langle 2,x\rangle\neq\mathbf{Z}[x]$看出.

例 5 找出 $\mathbf{Z}_6$ 的所有最大理想.

解: 由 § 4·3 例 4, $\mathbf{Z}_6$ 共有 4 个理想:零理想、单位理想、$I_1=\{[0],[2],[4]\}$和 $I_2=\{[0],[3]\}$. 由 § 4·4 例 5, $\mathbf{Z}_6/I_2\cong\mathbf{Z}_3$, 同样可证 $\mathbf{Z}_6/I_1\cong\mathbf{Z}_2$, 故 I_1、I_2 都是最大理想($\mathbf{Z}_2$, $\mathbf{Z}_3$ 是域).此外 $\mathbf{Z}_6$ 本身也是最大理想.

例 6 设 $R=\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbf{Z}\}$.

(1) $\langle\sqrt{2}\rangle$是什么样的集合?

(2) $\langle\sqrt{2}\rangle$是否最大理想?

解: R 是整环,所以$\langle\sqrt{2}\rangle=\{(a+b\sqrt{2})\sqrt{2}\mid a, b\in\mathbf{Z}\}=\{2b+a\sqrt{2}\mid a,b\in\mathbf{Z}\}$.即$\langle\sqrt{2}\rangle$包括一切偶数加整数乘$\sqrt{2}$的元素.

作 R 到 $\mathbf{Z}_2$ 的映射 φ 如下:

$$\varphi(a+b\sqrt{2})=\begin{cases}[0], & \text{当 } a \text{ 是偶数时,}\\ [1], & \text{当 } a \text{ 是奇数时.}\end{cases}$$

易证 φ 是满同态，其核为 $\langle\sqrt{2}\rangle$. 因而

$$R/\langle\sqrt{2}\rangle\cong \mathbf{Z}_2.$$

$\mathbf{Z}_2$ 是域，故 $\langle\sqrt{2}\rangle$ 是最大理想.

另证：设 I 是含 $\langle\sqrt{2}\rangle$ 的理想，$I\neq\langle\sqrt{2}\rangle$，$a+b\sqrt{2}\in I$，$a+b\sqrt{2}\notin\langle\sqrt{2}\rangle$，则 a 是奇数，$a-1$ 是偶数，$1=(a+b\sqrt{2})-[(a-1)+b\sqrt{2}]\in I$，因而对于任意 $r\in R$，$r=1\cdot r\in I$，即 $I=R$，说明含 $\langle\sqrt{2}\rangle$ 的理想除了 $\langle\sqrt{2}\rangle$ 外，只有单位理想，即 $\langle\sqrt{2}\rangle$ 是最大理想.

三、主理想环中的最大理想

在主理想环中，最大真理想有一个很好的判别方法：

定理 4 设 I 是非零主理想环，则真理想 $\langle p\rangle$ 是最大理想的充要条件是 p 为既约元.

证明：设 A 是 I 的最大理想，$A=\langle a\rangle$. 显然 $a\neq 0$，且是不可逆元(否则 $A=I$). 如果 a 是可约元，那末必有真因子 b，b 不是可逆元，故 $\langle b\rangle\neq I$. 另外，由于 $a\in\langle b\rangle$，$b\notin\langle a\rangle$，因而 $\langle a\rangle\subset\langle b\rangle\subset I$，说明 $A=\langle a\rangle$ 不是最大理想，矛盾. 所以 a 是既约元.

反之，假定 a 是既约元，则 a 不是可逆元，因而 $\langle a\rangle\neq I$. 这时 $\langle a\rangle$ 一定是最大理想. 因若不然，则有真理想 $B\supset\langle a\rangle$. 设 $B=\langle b\rangle$，那末 $a\in\langle b\rangle$，即有 $c\in I$，使 $a=bc$. c 不是可逆元(否则 $b\in\langle a\rangle$，$\langle b\rangle\subseteq\langle a\rangle$，矛盾)推出 a 是可约元.

证毕

由定理 2 和定理 4 得出：

推论 2　主理想环 I 的商环 $I/\langle p\rangle$ 是域的充要条件为 p 是既约元。

这里有一个重要特例：

推论 3　设 F 是域，$F[x]/\langle p(x)\rangle$ 是域的充要条件是 $p(x)$ 为既约多项式。

证明：$F[x]$ 是欧氏环，因而是主理想环，既约多项式是其既约元，由推论 2 得证。

例 7　求证 $\mathbf{Q}[x]/\langle x^2+2\rangle$ 是域，并求 $x+\langle x^2+2\rangle$ 的逆元。

解：x^2+2 是 $\mathbf{Q}[x]$ 的既约多项式。由推论 3，$\mathbf{Q}[x]/\langle x^2+2\rangle$ 是域，其元素形如 $f(x)+\langle x^2+2\rangle$。$x$ 与 x^2+2 互素，因而存在 $u(x)$，$v(x)\in\mathbf{Q}[x]$，使

$$x\cdot u(x)+(x^2+2)\cdot v(x)=1.$$

易见 $u(x)=-\dfrac{x}{2}$，$v(x)=\dfrac{1}{2}$ 满足上式。

$$\begin{aligned}&(x+\langle x^2+2\rangle)\left(-\frac{x}{2}+\langle x^2+2\rangle\right)\\&=-\frac{x^2}{2}+\langle x^2+2\rangle\\&=1-\frac{1}{2}(x^2+2)+\langle x^2+2\rangle\\&=1+\langle x^2+2\rangle.\end{aligned}$$

习　题　4·7

1. 找出 $\mathbf{Z}_{12}$ 的所有素理想与最大理想。
2. 域的同态除零同态外只有同构。
3. 设 p，q 是不同的素数，求证：$\langle[p]\rangle$ 是 $\mathbf{Z}_{pq}$ 的最大

理想和素理想。

4．可换环关于最大理想的商环是否总是域？

5．在$\mathbf{Q}[x]$中，找出包含$\langle x^2-2x+1\rangle$与$\langle x^2-1\rangle$的最大理想$I\neq\mathbf{Q}[x]$，并求$(x+1+I)(x^2-2+I)$与$(x+1+I)^{-1}$。

6．$\mathbf{Z}[i]$中以下理想哪些是最大理想？

$\langle 1\rangle$；$\langle 0\rangle$；$\langle i\rangle$；$\langle 1+2i\rangle$；$\langle 5\rangle$；$\langle 7\rangle$；$\langle 2+2i\rangle$。

7．设R是可换环，H是最大理想，求证：R/H是域的充要条件是H有性质$a\bar{\in} H\Rightarrow a^2\bar{\in} H$。

8．求证：$\mathbf{Z}_3[x]/\langle[1]x^2+[1]\rangle$是域。并求$[2]x+[2]+\langle[1]x^2+[1]\rangle$的逆元。

*§4·8 诺特环中的理想

本节介绍一类重要的环——诺特(Noether)[注]环中理想表为准素理想之交的性质。

一、准素理想

在整数环$\mathbf{Z}$中，理想$\langle 8\rangle$不是素理想，但有类似素理想的性质。如$ab\in\langle 8\rangle$，$a\bar{\in}\langle 8\rangle$，则$b$一定是偶数，因而$b^3\in\langle 8\rangle$。

定义1 设Q是可换环R的理想，具有以下性质：如果$ab\in Q$，$a\bar{\in} Q$，则有某个$b^n\in Q(n>0)$。这种理想Q称为R的准素理想。

显然素理想是准素理想。

注 E. Noether (1882—1935) 德国女数学家，抽象代数学科的奠基人之一。

例 1　$\mathbf{Z}[x,y]$中 $I=\langle x^2,\ xy,\ y^2\rangle$是准素理想．事实上，$I$包括且仅包括一切不含一次项及常数项的多项式．如果 $fg\in I$，$f\bar{\in} I$，那末 g 一定不含常数项，即 $g^2\in I$．同样也可看出，$\langle x^2,y\rangle$也是准素理想．

例 2　$\mathbf{Z}$ 中素数方幂生成的主理想$\langle p^k\rangle$显然是准素的；而若 $a\neq 0$，± 1 不是素数方幂，则$\langle a\rangle$不是准素的．事实上，设 $a=p_1^{k_1}\cdots p_n^{k_n}(n>1)$，取 $b=p_1^{k_1}$，$c=p_2^{k_2}\cdots p_n^{k_n}$，则 $bc=a\in\langle a\rangle, b\bar{\in}\langle a\rangle, c^m\bar{\in}\langle a\rangle$，$m=1,\ 2,\ \cdots$．所以 $\mathbf{Z}$ 中的准素理想都形如$\langle p^k\rangle$(p 为素数)和$\langle 0\rangle$，$\langle 1\rangle$．

以下考虑准素理想与素理想之间的关系．设 Q 是可换环 R 的准素理想，R 中某些元素的方幂可能在 Q 中，这样的元素组成的集合是

$$P=\{b\in R\,|\,存在\ n>0，使\ b^n\in Q\}.$$

P 称为 Q 的根，记为 $P=\sqrt{Q}$．显然 $Q\subseteq\sqrt{Q}$．如 $\mathbf{Z}$ 中，$\sqrt{\langle 8\rangle}=\sqrt{\langle 4\rangle}=\langle 2\rangle$．一般地 $\sqrt{\langle p^n\rangle}=\langle p\rangle$．$\mathbf{Z}[x,\ y]$ 中，$\sqrt{\langle x^2,xy,y^2\rangle}=\sqrt{\langle x^2,y\rangle}=\langle x,y\rangle$．$\langle p\rangle$和$\langle x,y\rangle$(由一切不含常数项的多项式组成)都是各自环中的素理想．一般地，有

定理 1　设 Q 是可换环 R 的准素理想，则 $P=\sqrt{Q}$ 是 R 的素理想．

证明：易证 P 是理想．此外设 $ab\in P$，则对某个 $n>0$，$(ab)^n\in Q$，即 $a^nb^n\in Q$．如果 $a\bar{\in} P$，那末 $a^n\bar{\in} Q$．因而 b^n 的某个方幂 $(b^n)^m\in Q$，即 $b^{mn}\in Q$，$b\in\sqrt{Q}=P$．即 P 为素理想．

证毕

若 $\sqrt{Q}=P$，则称 Q 为属于素理想 P 的准素理想．刚才看到，不同的准素理想可以属于同一素理想．

二、诺特环

在 $\mathbf{Z}$ 中，每个理想 $\langle a\rangle$ 可表为若干准素理想之交。如设 $a=p_1^{k_1}\cdots p_n^{k_n}$，则

$$\langle a\rangle=\langle p_1^{k_1}\rangle\cap\cdots\cap\langle p_n^{k_n}\rangle.$$

现在我们把这一性质推广到一类广泛的环。

定义 2 设 R 是有单位元的可换环，满足理想升链条件，即若 A_1，A_2，…是 R 的一系列理想，且 $A_1\subset A_2\subset\cdots$，则这个链只有有限项。这时，$R$ 称为诺特环。

以下给出诺特环的两个判别方法。

定理 2 在可换环 R 中，以下条件等价：

(1) R 是诺特环；

(2) R 满足理想的极大条件，即 R 的任意由理想组成的非空集 $\boldsymbol{F}$ 中一定有极大理想 M（M 不是 $\boldsymbol{F}$ 中任何理想的真子集）注。

(3) R 满足理想的有限生成条件，即 R 的每个理想都是由有限个元素生成的。

证明：(1)⇒(2)。任取 $A_1\in\boldsymbol{F}$，那末，或者 A_1 在 $\boldsymbol{F}$ 中极大，或者有 $A_2\in\boldsymbol{F}$，使 $A_1\subset A_2$，如果 A_2 不是极大的，则又有 $A_3\in\boldsymbol{F}$，使 $A_1\subset A_2\subset A_3$。由升链条件，这一过程经有限次必然停止，设为 n 项，则 A_n 是 $\boldsymbol{F}$ 中的一个极大理想。

(2)⇒(3)。假若 R 中理想 B 不是有限个元素生成的，则存在无限个元素 $a_i\in B(i=1,2,\cdots)$ 使 $A_i\subset A_{i+1}$，$A_i=\langle a_1,\cdots,a_i\rangle$，$i=1,2,\cdots$，取 $\boldsymbol{F}=\{A_i\mid i=1,2,\cdots\}\neq\phi$，则 $\boldsymbol{F}$ 中

注 极大理想不要与前节学的最大理想相混。

没有极大理想，矛盾。

(3)⇒(1)。设

$$A_1\subseteq A_2\subseteq A_3\subseteq\cdots\subseteq A_n\subseteq\cdots$$

是理想的包含链，取 $A=\bigcup_{i=1}^{\infty}A_i$，易见 A 是 R 的理想．由(3)，A 应当由有限个元素生成，设 $A=\langle a_1, \cdots, a_n\rangle$．假定 $a_1\in A_{i_1}, \cdots, a_n\in A_{i_n}$，取 $k=\max\{i_1, \cdots, i_n\}$．则 $A=\langle a_1, \cdots, a_n\rangle\subseteq A_k\subseteq A$，即 $A_k=A$，升链条件得证．

证毕

由有限生成条件立即可知，主理想环是诺特环，诺特环的理想和商环也是诺特环，而且可以证明〔称为希尔伯特(Hilbert)注 定理〕，诺特环上的多项式环也是诺特环．因而 $\mathbf{Z}$ 上的多项式环 $\mathbf{Z}[x]$、$\mathbf{Z}[x,y]$都是诺特环．

定义 3 设R是可换环，如果R的理想 I 能表为R的两个真包含 I 的理想之交，即

$$I=I_1\cap I_2,\quad I\subset I_1,\quad I\subset I_2,$$

则称 I 为R的可约理想．否则称为不可约理想．

素理想是不可约的，因为若素理想 $P=I_1\cap I_2$，$P\subset I_1$，$P\subset I_2$，则任取 $a_i\in I_i\backslash P$，$i=1, 2$，则 $a_1a_2\in P$，但 $a_1, a_2\overline{\in} P$，与素理想定义矛盾．然而不可约理想不一定是素理想，如 $\mathbf{Z}$ 中不可约理想$\langle 8\rangle$不是素理想，但是一个准素理想．一般地，有

定理 3 诺特环中每个不可约理想是准素理想．

证明：设理想 I 不是准素的，则存在 $c,d\in R$，使 $cd\in I$，

注 D. Hilbert (1862—1943) 德国人，本世纪最著名的数学家之一．1900年他在巴黎提出了著名的 23 个问题．

$c\overline{\in}I$，且对于 $k=1,2,\cdots$，$d^k\overline{\in}I$。取R中子集 $C_k=\{x|xd^k\in I\}$。显然 C_k 是R的理想(读者自证)，且

$$C_1\subseteq C_2\subseteq\cdots.$$

由于R是诺特环，故必有正整数 n，使 $C_n=C_{n+1}=\cdots$。设 $J=\{rd^n|r\in R\}$。显然 $I\subset I+J$。同时 $I\subset I+\langle c\rangle$。下面证明

$$I=(I+\langle c\rangle)\cap(I+J). \qquad (1)$$

事实上，任取右端集合的元素 b，由于 $cd\in I$，故 $I+\langle c\rangle$中每个元素与 d 之积在 I 中，于是 $bd\in I$。由于 $b\in I+J$，故 b 可表为 $b=a+rd^n$，$a\in I$，$r\in R$，因而 $bd=ad+rd^{n+1}$，即 $rd^{n+1}\in I$。又因 $C_{n+1}=C_n$，于是 $rd^n\in I$，$b\in I$，即 $I\supseteq(I+\langle c\rangle)\cap(I+J)$。反向的包含关系是明显的。由(1)式知，$I$ 可约。

证毕

注意：准素理想不一定是不可约的，如 $\mathbf{Z}[x,y]$中，$\langle x^2,xy,y^2\rangle=\langle x,y^2\rangle\cap\langle x^2,y\rangle$。

定理 4 诺特环中，每个理想可以表为有限个不可约理想的交。

证明：若不然，设 F 是不能表为有限个不可约理想之交的理想集，$F\neq\phi$。于是 F 中必有极大者，设为 M。显然 M 是可约的，因而存在理想 B 和 C，使 $M=B\cap C$，$M\subset B$，$M\subset C$，因为 M 是极大的，故 B 和 C 都可以表为有限个不可约理想之交。设

$$B=B_1\cap B_2\cap\cdots\cap B_r,\quad C=C_1\cap C_2\cap\cdots\cap C_s,$$

其中所有 B_i 和 C_i 都是不可约的。而

$$M=B_1\cap B_2\cap\cdots\cap B_r\cap C_1\cap C_2\cap\cdots\cap C_s,$$

可表为有限个不可约理想的交，矛盾。

证毕

推论 1 诺特环中每个理想可表为有限个准素理想的交。

下面考虑上述表示的唯一性。

假设理想 I 已表为准素理想的交

$$I = B_1 \cap B_2 \cap \cdots \cap B_k. \tag{2}$$

如果 $B_2 \cap \cdots \cap B_k \subseteq B_1$，则显然 B_1 可从(2)中舍去，这样，我们总可以使(2)式中每个 B_i 不包含在其它的交之中，这样得到的交称为无赘交。无赘交的表示中，不同的 B_i 可以属于同一素理想。这样，(2)又可分为若干组，每个组里的 B_i 同属于一个素理想。可以证明，同一组内的 B_i 之交仍是属同一素理想的准素理想，而不同组的 B_i 之交不是准素理想。于是(2)中可以归并为

$$I = C_1 \cap C_2 \cap \cdots \cap C_r \quad (r \leqslant k). \tag{3}$$

每个 C_i 是各自是属于不同素理想的准素理想。(3)无法再化成个数更少的准素理想的交。(3)中每个 C_i 称为 I 的一个最大准素分支。可以证明

定理 5 诺特环中，任意理想 I 可以由最大准素分支的无赘交表示，每种表示的这种分支数是 I 唯一确定的，各分支所属的素理想也是唯一确定的（分支本身并不是唯一确定的）。

如 $\mathbf{Z}[x,y]$中，

$$\langle x^2, xy\rangle = \langle x^2, xy, y^2\rangle \cap \langle x\rangle = \langle x^2, y\rangle \cap \langle x\rangle$$

都是$\langle x^2, xy\rangle$的最大准素分支表示，分支个数都是 2，而它们的分支分别属于素理想$\langle x, y\rangle$和$\langle x\rangle$。

本章提要

一、环的定义：具有 + 和 · 两种运算的代数系，关于 + 作成可换群，关于 · 作成半群，且 · 关于 + 有分配律。

二、整环：无零因子有单位元的非零可换环。

三、体：非零元可逆的环。

四、域：可换体。

五、子环：环的子集 $S\neq\phi$ 是子环的充要条件是 S 关于环的减法与乘法封闭。

六、理想：环的子集 $I\neq\phi$ 是环 R 的理想的充要条件是 I 关于减法封闭，且由 $a\in I$，$b\in R$ 得 $ab\in I$，$ba\in I$。

七、商环：设 I 是环 R 的理想，则商集 R/I 可以作成环，称为商环。

环关于同态核的商环同构于同态象。

八、素理想是具有这样性质的理想 P：若 $ab\in P$，则 a 或 b 至少有一个属于 P。

在适当条件下，P 是素理想等价于 P 对应的商环是整环。

九、最大理想：除理想本身和环外没有包含该理想的理想，叫做最大理想。

在适当条件下，最大理想等价于对应的商环是域。

十、唯一分解环：非零元作成唯一分解半群的环。

十一、主理想环：每个理想都是主理想的整环。

十二、欧氏环：具有类似于整数的带余除法性质的环。

欧氏环是主理想环，后者是唯一分解环。

复 习 题 四

1. 设环R的乘半群$\langle R,\cdot\rangle$具有唯一的左单位元e，求证e是单位元。

*2. 设a，b是环R的元素，$1-ab$可逆，求证：$1-ba$可逆。

3. 找出$\mathbf{Z}[\sqrt{2}]$的可逆元群。

*4. 设在有单位元的可换环中，求证：a是可逆元的充要条件是存在b，使$aba=a$，$ba^2b=1$。

5. 设p为素数，求证$\langle \mathbf{Z}_p^*,\cdot\rangle$中二阶元只有$[p-1]$。

*6. 设p为素数，求证：$(p-1)!\equiv-1(\bmod p)$注。

*7. 设I是有单位元环R的理想，设N是$1+I$中可逆元的集合，求证：N是R的可逆元群的正规子群。

8. 设I，J是环R的理想，$J\subseteq I$，求证：I/J是R/J的理想，$R/I\cong R/J\big/I/J$。

*9. 在主理想环R中，$a\in R$，设$T_a=\{x\mid x$与a互素$\}$，求证：$\{x+\langle a\rangle\mid x\in T_a\}$是半群$\langle R/\langle a\rangle,\cdot\rangle$的子群。

10. 设R是主理想环，$0\neq a\in R$，求证：只存在有限个理想包含a。

11. 求证：$\langle 3\rangle$是$\mathbf{Z}[i]$的素理想，而$\langle 2\rangle$不是素理想。

12. 设$F[0,1]$是$[0,1]$上的全体实函数的集合，求证：$F_0[0,1]=\{f(x)\in F[0,1]\mid f(0)=0\}$是最大理想。

13. 设$P_1\supseteq P_2\supseteq\cdots$是可换环$R$中素理想包含列。求证：

注 此题称为威尔逊（J. Wilson，1741—1793，英国人）定理。

$\bigcap\limits_{n=1}^{\infty} P_n$ 是R的素理想。

*14. 设P是体，σ是非零自同态. 求证：$S=\{\alpha \mid \sigma(\alpha)=\alpha\}$作成$P$的子体。

15. 设P是环R的素理想，S是R的子环，求证：除了$S\subseteq P$的情况外，$P\cap S$是S的素理想。

16. 设σ是环R到S的同态，P是S的素理想，求证：$\sigma[R]\subseteq P$的情况外，$\sigma^{-1}[P]$是R的素理想。

17. 设整环R与$\bar{R}$同态，求证$R[x]$与$\bar{R}[x]$同态，其同态核是什么？

18. 设$f(x)=x^n+a_1x^{n-1}+\cdots+a_n\in \mathbf{Z}[x]$，$\bar{f}(x)=[1]x^n+[a_1]x^{n-1}+\cdots+[a_n]\in \mathbf{Z}_p[x]$，$p$为素数。求证：若$\bar{f}(x)$在$\mathbf{Z}_p$上既约，则$f(x)$在$\mathbf{Z}$上既约。

19. 在整环R上的多项式环$R[x]$中，求证：$a_0+a_1x+\cdots+a_nx^n$既约当且仅当$a_n+a_{n-1}x+\cdots+a_0x^n$既约。

*20. 求证：有单位元环加法的交换律可由其他条件推出。

*21. 设环R有单位元1，元素u有右逆元（即有$x\in R$，$ux=1$），则以下条件等价：

(1) u的右逆元多于一个；

(2) u不是可逆元；

(3) u是左零因子，即存在$v\neq 0$，使$uv=0$。

*22. 设环R有单位元，$u\in R$，u的右逆元多于一个，求证u有无限多个右逆元。

23. 设R是环，A、B是其理想，求证：集合$\left\{\sum\limits_{i=1}^{n} a_i b_i \,\middle|\right.$

$a_i \in A$，$b_i \in B$，$n \geqslant 1\}$作成R的理想（记上述理想为AB）。

24．设R是可换环，A、B是环R的理想，求证：集合$\{r \in R \mid rb \in A$，对任意$b \in B\}$作成R的理想（记上述理想为$A:B$）；$A:B \supseteq A$；$(A:B)B \subseteq A$；$(A:B):A = A:AB = R$。

25．设R是有单位元1的环，含1的最小子环称为R的**素环**。求证：素环由形如$K1$（K为整数）的元素构成，它同构于Z或Zn。

*26．设R是有单位元1的环，R有一个子环是域F。求证：R的每个非零商环总有一个子环同构于F。

第五章　域

域是一种特殊的环。上章介绍了域的概念，本章进一步讨论域的基本性质，如域的扩张、分裂域、可分扩域、有限域以及其他一些初步知识，最后将略述伽罗华理论。

§5·1　域的基本性质

一、有限整环

域是整环，整环不一定是域。然而我们有

定理 1　有限整环是域。

证明：设 F 是有限整环，则 $\langle F^*,\cdot\rangle$ 是可换可消半群，自然是有限半群，根据 §3·2 定理 9，$\langle F^*,\cdot\rangle$ 是可换群，所以 F 是域。

证毕

二、域的特征

域 F 中包含两个可换群，一个是加群 $\langle F,+\rangle$，一个是非零乘群 $\langle F^*,\cdot\rangle$. 一个非零元同时是这两个群的元素. 元素在加群中的阶有以下性质：

定理 2　任意域 F 的非零元在加群 $\langle F,+\rangle$ 中有共同的阶.

证明：如果 F 的非零元在加群中都是无限阶的元素，自

然定理是对的。假定 F 的某一非零元 a 的阶为 n，任取 $b\in F^*$，只须证明 b 也是 n 阶元。事实上，

$$
\begin{aligned}
0&=(na)b=(a+a+\cdots+a)b\\
&=ab+ab+\cdots+ab=a(b+b+\cdots+b)\\
&=a(nb).
\end{aligned}
$$

F 中无非零因子，$a\neq 0$，所以 $nb=0$，b 的阶 $\leqslant a$ 的阶 n。同理可证 a 的阶 $n\leqslant b$ 的阶。即 b 的阶 $=n$。

证毕

定义 1 域 F 的非零元在加群 $\langle F,+\rangle$ 中的阶称为域 F 的特征。

定理 3 域 F 的特征或为素数或为 ∞。

证明：若 F 的特征是有限整数 p，p 如果是合数，$p=mn$，$1<m<p$，$1<n<p$。任取 F 中的非零元 a，则

$$0=pa=mna=(m\cdot 1)(n\cdot a).$$

（其中 1 是 F 的单位元）因而或者 $m\cdot 1=0$，或者 $n\cdot a=0$，与特征的定义矛盾，所以 p 是素数。

证毕

例 1 任何数域的特征都是 ∞，因为数 1 的任意正整数倍都不等于零。

例 2 在特征为 p 的域里，等式

$$(a+b)^p=a^p+b^p,\qquad (a-b)^p=a^p-b^p$$

成立。

证明：$(a+b)^p=a^p+C_p^1a^{p-1}b+C_p^2a^{p-2}b^2+\cdots+C_p^{p-1}ab^{p-1}$ $+b^p$，其中 $C_p^i=p\cdot\dfrac{(p-1)\cdots(p-i+1)}{1\cdot 2\cdots i}$，$i=1,2,\cdots,p-1$。

p 是素数，故 p 与 $1,2,\cdots,i$ 互素，所以 p 与 $1\cdot 2\cdots$

i 互素，而 $1\cdot 2\cdots i$ 整除 $p[(p-1)\cdots(p-i+1)]$ 因此 $1\cdot 2\cdots i$ 整除 $(p-1)\cdots(p-i+1)$。因而 C_p^1，C_p^2，…，C_p^{p-1} 都是 p 的倍数，上边展开式中间 $p-1$ 项等于零，故 $(a+b)^p=a^p+b^p$。

同理可证 $(a-b)^p=a^p-b^p$。

三、子域

定义 2 域 F 的非空子集 F_1 按 F 的运算作成域，则称 F_1 为 F 的子域，或 F 为 F_1 的扩域。

如果 F_1 是 F 的子域，则 F_1 为 F 的子环，并且 F_1 的非零元集 F_1^* 是 F^* 的子群。

任意域都有子域，因为至少自身是子域，其他子域称为真子域。如有理数域是实数域及复数域的真子域。

怎样判别子域呢？

定理 4 设 F_1 是域 F 的子集，F_1 含有非零元，F_1 是 F 子域的充要条件是：

(1) 若 a，$b\in F_1$，则 $a-b\in F_1$；

(2) 若 a，$b\in F_1$，$b\neq 0$，则 $ab^{-1}\in F_1$。

证明：必要性。

设 F_1 是 F 的子域，则 F_1 是 F 的子环，F_1 的零元即 F 的零元，且条件 1 成立。设 F_1 的单位元是 $1'$，则 $1'\cdot 1'=1'=1'\cdot 1$（1 是 F 的单位元），由于 $1'\neq 0$，故得 $1=1'\in F_1$。任取 F_1 中的非零元 b，设 b 在 F_1 和 F 中的逆元分别是 b' 和 b^{-1}，则 $bb'=1=bb^{-1}$，因而 $b^{-1}=b'\in F_1$。这样，由 a，$b\in F_1$，$b\neq 0$，可知 $b^{-1}\in F_1$，$ab^{-1}\in F_1$。

充分性。

由条件(2)，$\langle F_1^*, \cdot \rangle$是$\langle F^*, \cdot \rangle$的子群，因而$1 \in F_1$。由条件(1)，$\langle F_1, + \rangle$是$\langle F, + \rangle$的子群，故$0 \in F_1$。任取$a, b \in F_1$。若$a = b = 0$，则$ab = 0 \in F_1$；若$a$，$b$不全为零，不妨设$b \neq 0$，则$b \in F_1^*$，$b^{-1} = 1 \cdot b^{-1} \in F_1^*$，由条件(2)，$ab = a(b^{-1})^{-1} \in F_1$。从而$F_1$是$F$的子环。总之，$F_1$是$F$的子域。

证毕

由此不难得出以下的

定理 5 域的任意多个子域之交也是子域。

证明留给读者。

四、域的理想

我们知道，域没有真理想，只有两个平凡理想：零理想和单位理想。这个性质反映了域的本质。

定理 6 有单位元的非零可换环F当且仅当没有真理想时是域。

证明：必要性是显然的，下面证明充分性。

任取F的非零元a，由于$\langle a \rangle \neq \langle 0 \rangle$，故$\langle a \rangle = F$，因而$1 \in \langle a \rangle$。$\langle a \rangle$的元素都可以写成$ra$的形式，其中$r \in R$，故有$b \in R$，使$1 = ba = ab$，或$b = a^{-1}$。因而$F$是域。

证毕

域中既然只有两个(平凡)理想，这两个理想生成两个商环：

$$F/\langle 0 \rangle \cong F,\quad F/F \cong \{0\}.$$

而域的同态象总同构于一个商环，所以有

定理 7 域F的同态象或者是零环，或者同构于F。

五、素域

一个域 F 的所有子域的交 P 显然也是 F 的子域，这个子域是唯一的，它不可能有真子域，故称为 F 的素域。素域是最小的子域，其结构唯一地决定于域的特征。

定理 8 如果域 F 的特征是 ∞，则 $P\cong\mathbf{Q}$；如果 F 的特征是 p，则 $P\cong\mathbf{Z}_p$。

证明：分两种情况：

(1) 当 F 的特征是 ∞ 时，令 $P_1=\{(n\cdot1)(m\cdot1)^{-1}|m\neq0, m,n\in\mathbf{Z}\}$（其中 1 是 F 的单位元）。任取 $(n_1\cdot1)(m_1\cdot1)^{-1}$，$(n_2\cdot1)(m_2\cdot1)^{-1}\in P_1$，则

$$\begin{aligned}&(n_1\cdot1)(m_1\cdot1)^{-1}-(n_2\cdot1)(m_2\cdot1)^{-1}\\=&[(n_1\cdot1)(m_2\cdot1)-(n_2\cdot1)(m_1\cdot1)]\cdot[(m_1\cdot1)(m_2\cdot1)]^{-1}\\=&[(n_1m_2-n_2m_1)\cdot1]\cdot(m_1m_2\cdot1)^{-1}\in P_1;\end{aligned}$$

当 $(n_2\cdot1)(m_2\cdot1)^{-1}\neq0$，即 $n_2\neq0$ 时，有

$$\begin{aligned}&[(n_1\cdot1)(m_1\cdot1)^{-1}]\cdot[(n_2\cdot1)(m_2\cdot1)^{-1}]^{-1}\\=&[(n_1\cdot1)(m_2\cdot1)]\cdot[(m_1\cdot1)(n_2\cdot1)]^{-1}\\=&(n_1m_2\cdot1)(m_1n_2\cdot1)^{-1}\in P_1.\end{aligned}$$

这证明 P_1 是 F 的子域。由于 $1\in P_1$，所以显然 $P_1\subseteq P$。P 是素域，故 $P_1=P$。

作 $\mathbf{Q}$ 到 P 的映射 φ：

$$\varphi\left(\frac{n}{m}\right)=(n\cdot1)(m\cdot1)^{-1}.$$

易证 φ 是域同构，即 $P\cong\mathbf{Q}$。

(2) 当 F 的特征是 p 时，作 $\mathbf{Z}$ 到 P 的映射 φ：$\varphi(n)=n\cdot1$。φ 显然是环同态，其同态核 $K_\varphi=\{n|n\cdot1=0\}$。由于 F 的

特征是 p，所以 K_φ是 $\mathbf{Z}$中 p 的全体倍数的集合，即 $K_\varphi=\langle p\rangle$。而 $\varphi[\mathbf{Z}]=\{n\cdot 1\mid n\in\mathbf{Z}\}\subseteq P$。由环同态基本定理，$\mathbf{Z}_p=\mathbf{Z}/\langle p\rangle=\mathbf{Z}/K_\varphi\cong\varphi[\mathbf{Z}]$。$\mathbf{Z}_p$是域，所以 $\varphi[\mathbf{Z}]$也是域，且是 P 的子域，因而 $P=\varphi[\mathbf{Z}]$。而 $|P|=|\mathbf{Z}_p|=p$，P 是有限域。

证毕

因而，从同构的观点来看，任何域都不过是 $\mathbf{Q}$ 或 $\mathbf{Z}_p$（p 为素数）的扩域。

习 题 5·1

1. 当 p 为素数时，域 $\mathbf{Z}_p$ 的特征为何？

2. 在特征是 p 的域中，求证：

（1）$(a+b)^{p^n}=a^{p^n}+b^{p^n}$；

（2）$(a-b)^{p^n}=a^{p^n}-b^{p^n}$；

（3）$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$；

（4）$(n\cdot 1)^p=n\cdot 1$，其中 1 是域的单位元；

（5）$(a-b)^{p-1}=a^{p-1}+ab^{p-2}+\cdots+a^{p-2}b+b^{p-1}$。

3. 在 $\mathbf{Z}_7$ 中，求证：

（1）$[5^7]=[2^7]+[3^7]$；

（2）$[5^7]=[5]$。

4. 证明本节定理 5。

5. 求证：域与其子域特征相等。

6. 求证：高斯数域 $\{a+bi\mid a,b\in\mathbf{Q}\}$ 是 $\mathbf{C}$ 的子域。

7. 设 $F=\left\{\begin{pmatrix} a & b \\ -b & a\end{pmatrix}\middle|\, a,b\in\mathbf{R}\right\}$，求证：$F$ 关于方阵加法和乘法作成域，且同构于 $\mathbf{C}$。

8. 设 F 是特征为 p 的域，求证：子集 $F^p=\{a^p\mid a\in F\}$ 是

F 的子域。

9. 设 F 是特征为 p 的域，则 $a \to a^p$ 是 F 的自同态。试证明之。

10. 设 F 是特征为 p 的有限域，则 $a \to a^p$ 是 F 的自同构。

11. 设 F 是域，R 是非零子环，$F_1 = \{ab^{-1} | a, b \in R, b \neq 0\}$. 求证：$F_1$ 是 F 的子域，且是含 R 的最小子域。

§5·2 分 式 域

域是特殊的环，它有以下本质的性质：可换、无零因子、非零元可逆. 具有前两个性质的环（如整环）不一定是域，因为非零元不一定可逆. 那末，能不能作一个最小的域将已知环的非零元的逆元包括进去呢？或者说，环有没有最小扩域呢？这是可能的，例如整数环 $\mathbf{Z}$ 就有扩域 $\mathbf{Q}$. 这一节，我们将环扩充成域，其方法类似于将整数环扩充为有理数域的过程。

一、分式域是什么？

并非任何环都有扩域. 比如不可换环或有零因子环就没有扩域，因为任何域都没有零因子，而且关于乘法可换. 反过来，没有零因子的可换环是不是都有扩域呢？

定理 1 无零因子的非零可换环有扩域。

分析：设 R 是已知环，证明分以下几步：

（1）作出 $R \times R^*$ 的一个商集合 F；

（2）在 F 中规定代数运算 + 和 ·；

（3）证明 $\langle F, +, \cdot\rangle$ 是域；

（4）证明 F 的一个子环与 R 同构；

（5）利用环扩张定理，R 有扩域 $E\cong F$.

证明：（1）在积集 $R\times R^*=\{(a,b)\mid a,b\in R,b\neq 0\}$中规定关系～如下：

$$(a,b)\sim(c,d)\Longleftrightarrow ad=bc.$$

～满足等价关系三条件．事实上，

任取$(a,b)\in R\times R^*$，则 $ab=ba$，故 $(a,b)\sim(a,b)$．如果$(a,b)\sim(c,d)$，则 $ad=bc$，$cb=da$，$(c,d)=(a,b)$．如果$(a,b)\sim(c,d)$，$(c,d)\sim(e,f)$，则 $ad=bc$，$cf=de$，$(af-be)d=(ad)f-b(ed)=bcf-bcf=0$．$R$ 中无零因子，$d\neq 0$，故 $af=be$，$(a,b)\sim(e,f)$．

商集 $R\times R^*/\sim$记为 F．F 的元素是等价类：$[(a,b)]$．

（2）在 F 中规定：

$$[(a,b)]+[(c,d)]=[(ad+bc,bd)],$$

$$[(a,b)]\cdot[(c,d)]=[(ac,bd)].$$

它们都是 F 的代数运算．

事实上，由于$(a,b),(c,d)\in R\times R^*$，$b\neq 0$，$d\neq 0$，$R$ 无零因子，$bd\neq 0$，又 $ad+bc\in R$，$ac\in R$，因而$(ad+bc,bd)$，$(ac,bd)\in R\times R^*$，即以上两式右端属于 F．下面只须证明加法与乘法与代表元选取无关．

设$(a_1,b_1)\sim(a,b),(c_1,d_1)\sim(c,d)$，须证

$$(a_1d_1+b_1c_1,b_1d_1)\sim(ad+bc,bd),\qquad(1)$$

$$(a_1c_1,b_1d_1)\sim(ac,bd).\qquad(2)$$

由于 $a_1b=b_1a$，$c_1d=d_1c$，第一式乘 d_1d，第二式乘 b_1b，相加后得

$$a_1bd_1d+c_1db_1b=b_1ad_1d+d_1cb_1b,$$

或 $$(a_1d_1+b_1c_1)bd=b_1d_1(ad+bc),$$
因而(1)式成立.

将 $a_1b=b_1a$ 与 $c_1d=d_1c$ 相乘，得
$$a_1bc_1d=b_1ad_1c,\ \text{或}\ a_1c_1bd=b_1d_1ac.$$
得到(2)式.

(3) 加法适合交换律. 事实上,
$$[(a,b)]+[(c,d)]=[(ad+bc,bd)],$$
$$[(c,d)]+[(a,b)]=[(cb+da,db)],$$
而显然上两式相等.

加法适合结合律.

由于 $R^*\neq\phi$, 任意取定元素 $c\in R^*$.

$[(0,c)]$是$\langle F,+\rangle$的零元.

$[(-a,b)]$是$[(a,b)]$的负元.

乘法适合交换律和结合律，且关于加法适合分配律.

$[(c,c)]$是$\langle F,\cdot\rangle$的单位元.

$[(b,a)]$是$[(a,b)](\neq[(0,c)])$的逆元.

(以上几个断言的证明利用+和·的规定得出，留作练习)

因而 F 作成域.

(4) 作 R 到 F 的映射 φ 如下:
$$\varphi(a)=[(ac,c)],a\in R.$$
φ 显然是映射，而且是同态. 事实上,
$$\varphi(a+b)=[((a+b)c,c)]=[(ac+bc,c)]$$
$$=[(ac,c)]+[(bc,c)]=\varphi(a)+\varphi(b);$$
$$\varphi(ab)=[(abc,c)]=[(ac,c)][(bc,c)]$$
$$=\varphi(a)\varphi(b).$$
φ 是单射. 事实上，如果 $\varphi(a)=\varphi(b)$，则$[(ac,c)]=[(bc,$

c)], $(ac,c)\sim(bc,c)$, $ac^2=bc^2$, 推出$a=b$. $\varphi[R]=\{[ac,c]\mid a\in R\}$是 F 的子环（§ 4·4 定理 2 ），设为 R_1. 由于 φ 是单同态，故 $R\cong R_1$.

（5）显然 R 与 F 无公共元素，由环扩张定理(§4·4 定理 7),R 有扩环 $E\cong F$. F 是域，所以 E 也是域，是 R 的扩域.

证毕

上面只是抽象地决定了 R 的扩域 E 的存在，但 E 到底是什么样的？它的元素与 R 的元素有什么关系呢？

定理 2 E 由下面形式的元素组成：

$$ab^{-1},$$

其中 $a,b\in R$, $b\neq 0$.

证明：设 E 到 F 的同构映射为 ψ, ψ 在 R 上与定理 1 证明中的 φ 相同，即对 $a\in R$,

$$\psi(a)=\varphi(a)=[(ac,c)]\in R_1.$$

任取 $x\in E$, 设$[(a,b)]=\psi(x)$. 在 F 中，

$$[(a,b)]=[(ac,c)][(c,bc)]=[(ac,c)][(bc,c)]^{-1}$$

$$=\psi(a)\cdot\psi(b)^{-1}=\psi(ab^{-1}).$$

即 $\psi(x)=\psi(ab^{-1})$. ψ 是一一映射，故 $x=ab^{-1}$.

反之，任取 $a,b\in R$, $b\neq 0$, 则由于 E 是扩域，$ab^{-1}\in E$.

所以 $E=\{ab^{-1}\mid a,b\in R,\ b\neq 0\}$.

证毕

定义 1 设 R 是无零因子的非零可换环，E 是 R 的扩域，如果 E 由一切形如 ab^{-1} 的元素组成，其中 $a,b\in R$, $b\neq 0$, 则称 E 为 R 的分式域.

由定理 1 和定理 2 知，无零因子的可换环存在分式域.

例 1　有理数域 $\boldsymbol{Q}$ 是整数环 $\boldsymbol{Z}$ 的分式域。

证明：$\boldsymbol{Q}$ 是 $\boldsymbol{Z}$ 的扩域，$\boldsymbol{Q}$ 的每个元素形如 $\frac{m}{n}=mn^{-1}(m, n\in \boldsymbol{Z},\ n\neq 0)$。

例 2　实数域不是整数环的分式域。

证明：$\boldsymbol{R}$ 虽是 $\boldsymbol{Z}$ 的扩域，但 $\boldsymbol{R}$ 的元素不能全部写成 mn^{-1} 的形式，$\sqrt{2}$ 就是一例。

例 3　域 F 的分式域即其本身。

证明：F 是 F 的扩域，而 F 的每个元素 $a=a\cdot 1^{-1}$。

例 4　作出环 $R=\{a+b\sqrt{2}\mid a, b\in \boldsymbol{Z}\}$ 的一个分式域。

解：设 $F=\{\alpha+\beta\sqrt{2}\mid \alpha,\beta\in Q\}$。$F$ 显然作成域(是复数域 $\boldsymbol{C}$ 的子域)。R 是 F 的子环．F 中任意元素 $\alpha+\beta\sqrt{2}=\frac{m}{n}+\frac{l}{k}\sqrt{2}=\frac{mk+nl\sqrt{2}}{nk}=(mk+nl\sqrt{2})(nk+0\sqrt{2})^{-1}$，其中 $\alpha=\frac{m}{n}$，$\beta=\frac{l}{k}$，$m, n, k, l\in \boldsymbol{Z}, n\neq 0, k\neq 0$。所以 F 是 R 的分式域。

例 5　域 F 的多项式环 $F[x]$ 是无零因子的非零可换环。由一切形如 $\frac{f(x)}{g(x)}(g(x)\neq 0(x))$ 的所谓 F 上的有理分式组成的集合 $F(x)$ 中，规定类似于通常数域上的分式的运算，可知 $F(x)$ 作成 $F[x]$ 的扩域，称为 F 上的有理分式域．$F(x)$ 是 $F[x]$ 的分式域。

二、分式域的性质

一个环的分式域，从同构的意义上看，是唯一的。为了证

明这一点，须要证明

定理 3 设环 $R \cong \bar{R}$，Q 和 $\bar{Q}$ 分别是 R 及 $\bar{R}$ 的分式域，则 $Q \cong \bar{Q}$。

证明： 设 R 到 $\bar{R}$ 的同构映射为 φ。作 Q 到 $\bar{Q}$ 的映射 ψ 如下：

$$\psi(ab^{-1}) = \varphi(a) \cdot \varphi(b)^{-1}.$$

由于 φ 是满射，故 ψ 也是满射。此外，ψ 是单射。事实上，如果 $\psi(ab^{-1}) = \psi(cd^{-1})$，则

$$\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}, \quad \varphi(a)\varphi(d) = \varphi(b)\varphi(c),$$

$$\varphi(ad) = \varphi(bc).$$

φ 是一一映射，故 $ad = bc$，$ab^{-1} = cd^{-1}$。

ψ 是同态。事实上

$$\begin{aligned}
&\psi(ab^{-1} + cd^{-1}) \\
&= \psi((ad + bc)(bd)^{-1}) \\
&= \varphi(ad + bc)\phi(bd)^{-1} \\
&= [\varphi(a)\varphi(d) + \varphi(b)\varphi(c)]\varphi(b)^{-1}\varphi(d)^{-1} \\
&= \varphi(a)\varphi(b)^{-1} + \varphi(c)\varphi(d)^{-1} \\
&= \psi(ab^{-1}) + \psi(cd^{-1}).
\end{aligned}$$

$$\begin{aligned}
&\psi(ab^{-1} \cdot cd^{-1}) \\
&= \psi((ac)(bd)^{-1}) \\
&= \varphi(ac)\varphi(bd)^{-1} \\
&= \varphi(a)\varphi(c)\varphi(b)^{-1}\varphi(d)^{-1} \\
&= [\varphi(a)\varphi(b)^{-1}][\varphi(c)\varphi(d)^{-1}] \\
&= \psi(ab^{-1}) \cdot \psi(cd^{-1}).
\end{aligned}$$

总之，ψ 是 Q 到 $\bar{Q}$ 的同构，$Q \cong \bar{Q}$。

证毕

定理 3 中若取 $\bar{R}=R$，自然 $R\cong R$，因而有分式域的唯一性定理：

定理 4 设 Q 和 $\bar{Q}$ 都是环 R 的分式域，则 $\bar{Q}\cong Q$。

从例 2 可见，扩域不见得是分式域。分式域可以理解为最小扩域，即包含环 R 的最小的域，这就是

定理 5 如果域 F 是环 R 的扩域，则 F 包含 R 的分式域。

证明：在 F 中取集合

$$F_1=\{ab^{-1}\mid a, b\in R, b\neq 0\}.$$

F_1 含有 $1=bb^{-1}$，任取 ab^{-1}，$cd^{-1}\in F_1$，则

$$ab^{-1}-cd^{-1}=ab^{-1}dd^{-1}-cd^{-1}bb^{-1}=(ad-bc)(bd)^{-1}\in F_1,$$

设 $cd^{-1}\neq 0$，则

$$ab^{-1}\cdot(cd^{-1})^{-1}=ab^{-1}c^{-1}d=(ad)(bc)^{-1}\in F_1,$$

由 § 5·1 定理 4，F_1 是 F 的子域。R 显然是 F_1 的子环(因为 R 的元素 $a=a\cdot 1^{-1}$)，且由 F_1 元素的形式可见，F_1 是 R 的分式域。

证毕

习 题 5·2

1. 求证：高斯数域 $\mathbf{Q}(i)$ 是高斯数环 $\mathbf{Z}[i]$ 的分式域。
2. 求证：$\mathbf{Q}$ 是偶数环 $\boldsymbol{E}$ 的分式域。
3. 求证定理 1 证明中(3)的几个断言。
4. 设 $R=\left\{\frac{m}{2^n}\middle| m\in\mathbf{Z}, n\in\boldsymbol{N}\right\}$，求证 R 是 $\mathbf{Q}$ 的子环，写出 R 的分式域。

§ 5·3 域的单扩张

设 F 是域 E 的子域，M 是 E 的子集，包含 F 和 M 的子域一定存在（例如 E 就是这样的子域），满足这个条件的子域的交也是 E 的子域，记为 $F(M)$，它是包含 F 和 M 的最小子域。如果 M 是单元素集 $\{c\}$，那末 $F(c)$ 称为 F 的单扩域。单扩域是最简单的扩域，又分为两种，即单代数扩域和单超越扩域，这要看 c 是代数元还是超越元。

一、单代数扩域

若 c 是 F 的代数元，则 $F(c)$ 称为单代数扩域。

$F(c)$ 包含 c 和 F，因而 $F(c)$ 包含一切 $f(c)$，其中 $f(x)$ 是 F 上的任一多项式，即 $F(c)\supseteq F[c]$。

定理 1 如果 c 是 F 的代数元，则 $F(c)=F[c]$。

分析：只须证明 $F[c]$ 是 E 的子域。为此，要证 $F[x]$ 到 $F[c]$ 的同态核 N 是既约多项式 $p(x)$ 生成的最大理想，则 $F[c]\cong F[x]/N$ 是域。

证明：$F[x]$ 到 $F[c]$ 的映射

$$\varphi(f(x))=f(c)\quad (f(x)\in F[x])$$

是同态（见 § 4·5 定理 2）.同态核设为 N，故

$$F[x]/N\cong F[c]. \tag{1}$$

N 是 $F[x]$ 的理想，由以 c 为根的多项式组成。F 是域，$F[x]$ 是主理想环，N 是主理想，设 $N=\langle p(x)\rangle$。$p(x)\in N$，$p(c)$

$=0$，故 $p(x)$ 不是零次多项式．$p(x)\neq 0(x)$，因为否则 $N=\langle 0(x)\rangle=\{0(x)\}$，推出 c 是 F 的超越元，矛盾．总之，$p(x)$ 次数$\geqslant 1$．如果 $p(x)$ 在 F 上可约，设 $p(x)=p_1(x)p_2(x)$，$p_1(x)$和 $p_2(x)$都是 $p(x)$ 的真因子．由于

$$0=p(c)=p_1(c)p_2(c),$$

E 中无零因子，所以 $p_1(x)$和$p_2(x)$至少有一属于 $N=\langle p(x)\rangle$，于是 $p(x)\mid p_1(x)$或 $p(x)\mid p_2(x)$，出现矛盾，所以$p(x)$是 F上既约多项式，因而 N 是 $F[x]$的最大理想，$F[x]/N$ 是域．由(1)式，$F[c]$是域．

$F[c]$是含 F 和 c 的域，根据 $F(c)$的定义，$F(c)\subseteq F[c]$，又由前面所讲，$F(c)\supseteq F[c]$，故 $F(c)=F[c]$．

证毕

$F[c]$ 是 E 中包含 F 和 c 的最小子环，或者说是 F 由 c 生成的单扩环．定理 1 说明，对于 E 的子域 F 的代数元来说，单扩域刚好和单扩环相同，这是单代数扩域的特点．

定义 1 设 F 是域 E 的子域，$c\in E$ 是 F 的代数元，F 上以 c 为根首项系数为 1 （F 的单位元）的最低次多项式

$$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$$

称为 c 在 F 上的极小多项式．

那么极小多项式是不是唯一呢？有什么重要性质呢？

定理 2 F 的代数元 c 的极小多项式 $p(x)$是 $F[x]$ 中既约多项式，且是唯一的．

证明：显然，$p(x)$ 不可能是 $0(x)$ 或零次多项式．假如 $p(x)$可约，$p(x)=p_1(x)p_2(x)$，$p_1(x)$ 和 $p_2(x)$ 次数都低于 $p(x)$的次数，那么 $0=p(c)=p_1(c)p_2(c)$，由于 $p_1(c)$，$p_2(c)\in E$，E 中无零因子，故 c 又是一个较低次的多项式 $p_1(x)$或

$p_2(x)$的根，与 $p(x)$的极小性矛盾。所以，$p(x)$ 是 F 上的既约多项式。

如果 $q(x)$也是 c 的极小多项式，若 $q(x)\neq p(x)$，则 $q(x)-p(x)\neq 0(x)$，次数低于 n ($p(x)$与 $q(x)$ 首项相同)，$q(c)-p(c)=0$，即 c 是一个较低次的多项式的根，矛盾。所以 c 的极小多项式是唯一的。

证毕

注意： 超越元是不存在极小多项式的，因为它不是 $F[x]$ 中任何非零多项式的根。

定义 2 在定义 1 中 $p(x)$的次数 n，称为 c 在 F 上的次数。

例 1 试求：i 在 $\boldsymbol{R}$ 上的次数、$\sqrt{2}$ 在 $\boldsymbol{Q}$ 上的次数及 $\sqrt{2}+i$ 在 $\boldsymbol{R}$ 和 $\boldsymbol{Q}$ 上的次数。

解： i 在 $\boldsymbol{R}$ 上的极小多项式是 x^2+1，为二次多项式，所以 i 在 $\boldsymbol{R}$ 上的次数为 2 。

$\sqrt{2}$ 在 $\boldsymbol{Q}$ 上的极小多项式是 x^2-2，所以 $\sqrt{2}$ 是 $\boldsymbol{Q}$ 上的 2 次元。

$\sqrt{2}+i$ 是 $\boldsymbol{R}$ 上的 2 次元，因为其极小多项式是 $x^2-2\sqrt{2}x+3$。但 $\sqrt{2}+i$ 不是 $\boldsymbol{Q}$ 上的 2 次元，而是 4 次元。事实上，设 $c=\sqrt{2}+i$，则

$$c^2=2+2\sqrt{2}i+(-1)=1+2\sqrt{2}i.$$

$$c^2-1=2\sqrt{2}i, \qquad (c^2-1)^2=-8,$$

$$c^4-2c^2+1=-8.$$

c 是多项式 $p(x)=x^4-2x^2+9$ 的根。容易证明（例如用待定系数法），$p(x)$是 $\boldsymbol{Q}[x]$中的既约多项式，必定是 c 的极小多项式，这因为有

定理 3 设 c 是 F 的代数元，$p(x)$ 是首项系数为 1 的既约多项式，$p(c)=0$，则 $p(x)$是 c 的极小多项式。

证明：以 c 为根的多项式集 N 是 $F[x]$ 中的理想（见定理 1 的证明），它是主理想，设 $N=\langle q(x)\rangle$，则$q(x)\mid p(x)$，$p(x)$是既约的，故 $q(x)$与 $p(x)$相伴，因而 $N=\langle p(x)\rangle$，$p(x)$ 是 N 中次数最低者，即 c 的极小多项式。

证毕

二、由代数元决定的单代数扩域

设 c 是域 E 的子域 F 的代数元，c 唯一决定极小多项式 $p(x)$，由 $p(x)$可以构造出 $F(c)$来。

定理 4 $F(c)\cong F[x]/\langle p(x)\rangle$，其中 $p(x)$ 是 c 的极小多项式。

证明：在定理 1 的证明中已经知道 $F(c)=F[c]\cong F[x]/N$，其中 N 是一个主理想，$N=\langle p(x)\rangle$，$p(x)$是一个既约多项式，$p(c)=0$，设 $f(x)\in F[x]$，$f(c)=0$，则 $f(x)\in N$，$p(x)\mid f(x)$，$f(x)$的次数将不低于 $p(x)$的次数，所以 $p(x)$ 是 c 的极小多项式（不妨取 $p(x)$的首项系数为 1）。

证毕

例 2 $\boldsymbol{R}(i)\cong\boldsymbol{R}[x]/\langle 1+x^2\rangle$

证明：i 在 $\boldsymbol{R}$ 的极小多项式为 $1+x^2$，故由定理 4 得证。

仅知道单代数扩域 $F(c)$ 的同构象 $F[x]/\langle p(x)\rangle$ 还是不够的，因为 $F(c)$的元素还没有明确的认识，下面的定理介绍 $F(c)$中元素的形式。

定理 5 设 c 是域 F 的 n 次元，则 $F(c)$中每个元素可唯一地表为以下形式：

$$a_0 + a_1 c + a_2 c^2 + \cdots + a_{n-1} c^{n-1}, \tag{2}$$

其中各 $a_i \in F$。即

$F(c) = \{a_0 + a_1 c + \cdots + a_{n-1} c^{n-1} \mid a_i \in F,\ i = 0, 1, \cdots, n-1\}$。

证明：由于 $F(c) = F[c]$，$F[c]$中元素形如

$$\alpha = b_0 + b_1 c + \cdots + b_m c^m.$$

用 $p(x)$对 $f(x) = b_0 + b_1 x + \cdots + b_m x^m$ 进行带余除法，设 $f(x) = q(x)p(x) + r(x)$，其中

$$r(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

$$f(c) = q(c)p(c) + r(c),$$

因为 $p(c) = 0$，故

$$\alpha = f(c) = r(c) = a_0 + a_1 c + \cdots + a_{n-1} c^{n-1}.$$

下面证明(2)式的唯一性。设

$$a_0 + a_1 c + \cdots + a_{n-1} c^{n-1} = b_0 + b_1 c + \cdots + b_{n-1} c^{n-1},$$

则 c 是多项式

$$d(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$$

的根，因而 $p(x) \mid d(x)$，所以 $d(x) = 0(x)$，$a_i = b_i$，$i = 0, 1, \cdots, n-1$。

反之，任取 $a_0, a_1, \cdots, a_{n-1} \in F$，则

$$a_0 + a_1 c + \cdots + a_{n-1} c^{n-1} \in F[c] = F(c).$$

证毕

如果 F 的代数元 α 和 β 有同一极小多项式，那末 $F(\alpha)$ 和 $F(\beta)$有什么关系呢？

定义 3 设 E_1 和 E_2 都是 F 的扩域，假如存在同构 $E_1 \cong E_2$，它使得 F 中的元素保持不动，则称 E_1 和 E_2 关于 F 等价。

定理 6 设 α 和 β 在 F 上有同一极小多项式 $p(x)$，则

$F(\alpha)$和 $F(\beta)$ 关于 F 等价。

证明：由定理 4，

$$F(\alpha)\cong F[x]/\langle p(x)\rangle\cong F(\beta).$$

因而 $F(\alpha)\cong F(\beta)$。

设 φ 是 $F(\alpha)$到 $F[x]/\langle p(x)\rangle$的同构，ψ 是 $F(\beta)$到 $F[x]/\langle p(x)\rangle$的同构，那末 $\sigma=\psi^{-1}\varphi$ 是 $F(\alpha)$到 $F(\beta)$ 的同构。当 $a\in F$时，

$$\varphi(a)=a+\langle p(x)\rangle=\psi(a),$$

即 $\sigma(a)=\psi^{-1}(\varphi(a))=a$。$\sigma$ 在 F 上是恒等变换。$F(\alpha)$ 和 $F(\beta)$ 关于 F 等价。

证毕

如 i 和 $-i$ 在 $\boldsymbol{R}$ 上的极小多项式都是 $1+x^2$。$\boldsymbol{R}(i)=\{a+bi\mid a,b\in\boldsymbol{R}\}$，$\boldsymbol{R}(-i)=\{a-bi\mid a,b\in\boldsymbol{R}\}$，映射 $a+bi\to a-bi$ 是同构映射，且保持 $\boldsymbol{R}$ 中元素不动，所以 $\boldsymbol{R}(i)$和 $\boldsymbol{R}(-i)$等价。

但是同一域的两个同次代数元生成的单扩域不一定同构。如 i 和$\sqrt{2}$都是 $\boldsymbol{Q}$ 的 2 次元。

$$\boldsymbol{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\boldsymbol{Q}\},$$

$$\boldsymbol{Q}(i)=\{a+bi\mid a,b\in\boldsymbol{Q}\}.$$

但它们不同构。因为否则，设 i 的同构象为 $a+b\sqrt{2}$，由于 1 的象必须是 1（单位元的同构象仍是单位元），0 的象仍是 0，$-1=0-1$ 的象也是 -1，$i^2=-1$，故 $(a+b\sqrt{2})^2=-1$，即 $a^2+2\sqrt{2}ab+2b^2=-1$，$a^2+2b^2=-1$，矛盾。

例 3 在 $\boldsymbol{Q}(\sqrt[3]{2})$ 中求 $1+\sqrt[3]{2}+\sqrt[3]{4}$ 的逆元。

解：$\sqrt[3]{2}$ 在 $\boldsymbol{Q}$ 上的极小多项式是 x^3-2。所以

$$\boldsymbol{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{4}\mid a,b,c\in\boldsymbol{Q}\}.$$

设$(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}=a+b\sqrt[3]{2}+c\sqrt[3]{4}$。则

$$1=(1+\sqrt[3]{2}+\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4})$$
$$=(a+2b+2c)+(a+b+2c)\sqrt[3]{2}+(a+b+c)\sqrt[3]{4}.$$

对比系数可得 $a=-1, b=1, c=0$，所以 $(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}$ $=-1+\sqrt[3]{2}$。

另解：$\mathbf{Q}(\sqrt[3]{2})\cong\mathbf{Q}[x]/\langle x^3-2\rangle$。$1+\sqrt[3]{2}+\sqrt[3]{4}$ 的同构象是 $1+x+x^2+\langle x^3-2\rangle$。$1+x+x^2$ 与 x^3-2 互素，易知

$$(1+x+x^2)(-1+x)-(x^3-2)=1,$$

所以$(1+x+x^2)+\langle x^3-2\rangle$的逆元是$(-1+x)+\langle x^3-2\rangle$，在 $\mathbf{Q}(\sqrt[3]{2})$中$(-1+x)+\langle x^3-2\rangle$对应元素是$-1+\sqrt[3]{2}$。所以

$$(1+\sqrt[3]{2}+\sqrt[3]{4})^{-1}=-1+\sqrt[3]{2}.$$

例 4　i 是 $\mathbf{R}$ 的 2 次元，所以 $\mathbf{R}(i)$ 的元素唯一地表为 $a+bi$ 的形式，其中 $a, b\in\mathbf{R}$，即 $\mathbf{C}=\mathbf{R}(i)$。

$\sqrt{2}+i$是$\mathbf{Q}$的 4 次元，故$\mathbf{Q}(\sqrt{2}+i)$中元素唯一地表为 $a+b(\sqrt{2}+i)+c(\sqrt{2}+i)^2+d(\sqrt{2}+i)^3$ 的形式，其中 $a, b, c, d\in\mathbf{Q}$。

三、由既约多项式决定的单代数扩域

刚才，我们由域 F 的一个代数元唯一地决定了代数扩域。这要求 F 有一个已知的扩域 E，但是如果没有给出这样的扩域 E，也不知道这个代数元，仅给出 F 上的一个既约多项式，能不能得到一个代数扩域，并使其包含这个既约多项式的一个根呢？回答是肯定的：

定理 7　设 $p(x)$是域 F 上的首项系数为 1 的既约多项式，则存在 F 的单代数扩域 $F(\alpha)$，使 $p(x)$是 α 的极小多项式，且 $F(\alpha)\cong F[x]/\langle p(x)\rangle$。

分析：作一个域 $\bar{E}$，使其有一个子域 $\bar{F}\cong F$，由环扩张定理，F 有一个扩域 $E\cong\bar{E}$，E 为所求。

证明：$p(x)$为既约多项式，$\langle p(x)\rangle$是 $F[x]$的最大理想，所以 $\bar{E}=F[x]/\langle p(x)\rangle$是域，其元素形如 $f(x)+\langle p(x)\rangle(f(x)\in F[x])$。

设 φ 是 $F[x]$到 $\bar{E}$ 的自然同态：

$$\varphi(f(x))=f(x)+\langle p(x)\rangle.$$

设$\varphi[F]=\bar{F}$，因而 $\bar{F}$ 是 $\bar{E}$ 的子环（因为 F 是 $F[x]$ 的子环）。若 $a\neq b$，则 $p(x)\nmid a-b$，因而

$$a+\langle p(x)\rangle\neq b+\langle p(x)\rangle,$$

所以 φ 看作 F 到 $\bar{F}$ 的映射时，是同构，即 $F\cong\bar{F}$，$\bar{F}$ 是域。

F 显然与 $\bar{E}$ 无共同元素，由环扩张定理，(§ 4·4 定理 7)，F 有扩环 $E\cong\bar{E}$，$\bar{E}$ 是域，所以 E 也是域。设 E 到 $\bar{E}$ 的同构映射为 ψ，在 F 中 ψ 与 φ 相同。设 $x+\langle p(x)\rangle\in\bar{E}$ 在 E 中对应元素为 α，即 $\psi(\alpha)=x+\langle p(x)\rangle$。

设 $p(x)=a_0+a_1x+\cdots+a_nx^n$，那末

$$\begin{aligned}\psi(p(\alpha))&=\psi(a_0)+\psi(a_1)\psi(\alpha)+\cdots+\psi(a_n)\psi(\alpha)^n\\&=\varphi(a_0)+\varphi(a_1)(x+\langle p(x)\rangle)+\cdots\\&\quad+\psi(a_n)(x+\langle p(x)\rangle)^n\\&=(a_0+\langle p(x)\rangle)+(a_1+\langle p(x)\rangle)(x+\langle p(x)\rangle)\\&\quad+\cdots+(a_n+\langle p(x)\rangle)(x+\langle p(x)\rangle)^n\\&=(a_0+a_1x+\cdots+a_nx^n)+\langle p(x)\rangle\\&=\langle p(x)\rangle\ (\bar{E}\text{ 的零元}).\end{aligned}$$

所以 $p(\alpha)=0$，即 α 是 $p(x)$的根，是 F 的代数元。由定理 3，$p(x)$是 α 的极小多项式。

下面证明 $F(\alpha)=E$。

首先，由于 $F\subseteq E$，$\alpha\in E$，E是F的扩域，故$F(\alpha)\subseteq E$。另一方面，任取$\beta\in E$，设$\psi(\beta)=f(x)+\langle p(x)\rangle$，假定$f(x)=b_0+b_1x+\cdots+b_mx^m$，则

$$\begin{aligned}\psi(f(\alpha))&=\psi(b_0)+\psi(b_1)\psi(\alpha)+\cdots+\psi(b_m)\psi(\alpha)^m\\&=(b_0+\langle p(x)\rangle)+(b_1+\langle p(x)\rangle)(x+\langle p(x)\rangle)\\&\quad+\cdots+(b_m+\langle p(x)\rangle)(x+\langle p(x)\rangle)^m\\&=(b_0+b_1x+\cdots+b_mx^m)+\langle p(x)\rangle\\&=f(x)+\langle p(x)\rangle=\psi(\beta).\end{aligned}$$

由于ψ是一一映射，故$\beta=f(\alpha)\in F(\alpha)$。

因而$E=F(\alpha)$是单代数扩域。

证毕

例5 $1+x^2$是$\boldsymbol{R}[x]$中的既约多项式，由定理5，存在$\boldsymbol{R}$的单代数扩域$\boldsymbol{R}(\alpha)$包含$1+x^2$的根α，改记$i=\alpha$，$\boldsymbol{C}=\boldsymbol{R}(i)$。由$1+x^2$这个多项式得到复数域。这就是最初柯西(Cauchy)创造的方法。定理7是克伦奈克尔(Kronecker)注推广柯西的方法所得到的一般结果。

例6 $p(x)=[1]x^2+[1]x+[1]$是$\boldsymbol{Z}_2[x]$中的既约多项式，这因为$p(x)$如果可约，那末必有一次因子，因而在$\boldsymbol{Z}_2$中有根，但$p([0])=[1]$，$p([1])=[1]$，所以$p(x)$既约。由定理7，存在$\boldsymbol{Z}_2$的单代数扩域$\boldsymbol{Z}_2(\alpha)$，包含$p(x)$的一个根α。又由定理5，$\boldsymbol{Z}_2(\alpha)$有元素：

$$[0]+[0]\alpha,\ [0]+[1]\alpha,\ [1]+[0]\alpha,\ [1]+[1]\alpha.$$

即$[0]$，$[1]\alpha$，$[1]$，$[1]+[1]\alpha$，共四个元素，其运算表如下：

注 A. Cauchy (1789—1857)法国数学家. L. Kronecker (1823—1891)德国数学家。

+	[0]	[1]	[1]a	[1]+[1]a
[0]	[0]	[1]	[1]a	[1]+[1]a
[1]	[1]	[0]	[1]+[1]a	[1]a
[1]a	[1]a	[1]+[1]a	[0]	[1]
[1]+[1]a	[1]+[1]a	[1]a	[1]	[0]

•	[0]	[1]	[1]a	[1]+[1]a
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[1]a	[1]+[1]a
[1]a	[0]	[1]a	[1]+[1]a	[1]
[1]+[1]a	[0]	[1]+[1]a	[1]	[1]a

如求$([1]+[1]a)([1]+[1]a)$，只须注意$p(a)=0$，即$[1]a^2=-[1]a-[1]=[1]a+[1]$（在$\mathbf{Z}_2$中，$[1]=-[1]$），所以

$$([1]+[1]a)([1]+[1]a)=[1]+[1]a+[1]a+[1]a^2$$
$$=[1]+[1]a^2=[1]+[1]a+[1]=[1]a.$$

四、单超越扩域

现在讨论单超越扩域，即扩域$F(a)$，其中a是F的超越元。

定理 8 设E是F的扩域，$a\in E$是F的超越元，则$F(a)$与F上的有理分式域$F(x)$同构.（见§5·2例5）

证明：作$F[x]$到E的映射φ：

$$\varphi(f(x))=f(a).$$

显然，φ是同态，其核是零．事实上，设$\varphi(f(x))=0$，则$f(a)=0$．a是超越元，故$f(x)=0(x)$．因而φ是同构，

$$\varphi(F[x]) = F[\alpha] \cong F[x].$$

所以，这两环的分式域也同构（§5·2 定理3）．$F[x]$ 的分式域是 $F(x)$，$F[\alpha]$的分式域是包含 F 和 α 的域，而单扩域 $F(\alpha)$ 是包含 F 和 α 的最小域，故 $F(\alpha) \subseteq F[\alpha]$ 的分式域．

另一方面，由于 $F \subseteq F(\alpha)$，$\alpha \in F(\alpha)$，故 $F[\alpha] \subseteq F(\alpha)$．由§5·2 定理5，$F[\alpha]$的分式域$\subseteq F(\alpha)$．即 $F(\alpha)$为 $F[\alpha]$ 的分式域．所以 $F(\alpha) \cong F(x)$．

证毕

推论1 一个域的任意两个单超越扩域都同构，且关于 F 等价．

所以，从同构的观点看，域 F 的单超越扩域只有一个，即 F 上的有理分式域 $F(x)$．

例7 π 是 $\mathbf{Q}$ 的超越元，故

$$\mathbf{Q}(\pi) = \left\{ \frac{a_0 + a_1\pi + \cdots + a_n\pi^n}{b_0 + b_1\pi + \cdots + b_m\pi^m} \middle| a_i,\ b_j \in \mathbf{Q}, n, m \geqslant 0 \right\}.$$

习　题　5·3

1. 找出下列复数在 $\mathbf{Q}$ 上的极小多项式：

(1) $1+\sqrt{2}$；　　(2) $\sqrt{2}+\sqrt{3}$；

(3) $1+i$；　　(4) $\sqrt{1+\sqrt[3]{2}}$．

2. 写出上面4个元素对应单扩域中元素的一般形式．

3. 写出 $\mathbf{Z}_3$上的一个三次既约多项式．由此证明存在含27个元素的域．

4. 以下元素关于对应的域是代数元还是超越元？

(1) $i, \mathbf{Q}$；(2) $1+i, \mathbf{R}$；(3) $\sqrt{\pi}, \mathbf{Q}$；(4) $\sqrt{\pi}, \mathbf{R}$；(5) $\sqrt{\pi}, \mathbf{Q}(\pi)$；(6) $\sqrt{\pi}+1, \mathbf{Q}(\pi^2)$；(7) $\pi^2, \mathbf{Q}$．

5. 设 α 是域 F 的超越元，$\beta\in F(\alpha)$，但 $\beta\overline{\in}F$，求证 β 也是 F 的超越元。

6. 求证：$p(x)=[1]x^3+[1]x^2+[1]$ 是 $\mathbf{Z}_2[x]$ 中的既约多项式。求作单扩域，使其包含 $p(x)$ 的根。

7. 设 F 是域 E 的子域，α 是 F 的代数元，α 在 F 上的极小多项式设为 $p(x)$，α 在 E 上的极小多项式设为 $q(x)$。求证：在 $E[x]$ 中，$q(x)\mid p(x)$。

8. 找出下列元素在给定域的逆元：

(1) $1+\sqrt[3]{2}\in\mathbf{Q}(\sqrt[3]{2})$；

(2) $5+6\varepsilon\in\mathbf{Q}(\varepsilon)$，其中 ε 是 x^2+x+1 的根；

(3) $[1]\alpha^2\in\mathbf{Z}_3(\alpha)$，其中 α 的极小多项式为 $[1]x^3+[2]x+[1]$；

(4) $\sqrt[3]{5}+1\in\mathbf{Q}(\sqrt[3]{5})$。

9. 找出 $3x+4+\langle x^2-2\rangle$ 与 $5x-6+\langle x^2-2\rangle$ 在 $\mathbf{Q}[x]/\langle x^2-2\rangle$ 中的和与积。

§5·4　有限扩域与代数扩域

在线性代数中学过数域上的向量空间(或线性空间)，现在我们在一般的域上建立向量空间，由此出发，可以更清楚地了解扩域的结构。

一、向量空间

定义1　设 E 是加群，F 是域。假定存在 $F\times E$ 到 E 的映射：$(\lambda,a)\rightarrow\lambda a$，满足以下四条性质：

(1) 设 1 是 F 的单位元，$a\in E$，则 $1\cdot a=a$。

(2) $\lambda(a+b)=\lambda a+\lambda b(\lambda\in F,a,b\in E)$；

(3) $(\lambda+\mu)a=\lambda a+\mu a(\lambda,\mu\in F,a\in E)$；

(4) $(\lambda\mu)a=\lambda(\mu a)(\lambda,\mu\in F,a\in E)$。

这时，称E为F上的向量空间。

线性代数中数域上的向量空间概念，例如线性相关、无关、基、维数、线性组合等可以直接运用。

二、有限扩域

如果E是F的扩域，则E是F上的向量空间。这时，如果E关于F的向量空间是有限维的，即在E中存在有限个线性无关的元素，E的每个元素都是它们的线性组合，则称E是F的有限扩域，向量空间E的维数称为扩域E在F上的次数，记为$[E:F]$。显然$[E:E]=1$。

如果E是F上的无限维空间，则称E是F的无限扩域，记为$[E:F]=\infty$。

例1 $[\boldsymbol{C}:\boldsymbol{R}]=2$。

证明：$\boldsymbol{C}=\{a+bi\mid a,b\in\boldsymbol{R}\}$，因而$\boldsymbol{C}$中元素可由1和$i$线性表示。而1和$i$线性无关，这因为如果$\lambda\cdot 1+\mu\cdot i=0$，$(\lambda,\mu\in\boldsymbol{R})$则$\lambda+\mu i=0,\lambda=\mu=0$。所以1，$i$是$\boldsymbol{C}$在$\boldsymbol{R}$上的一组基。即$[\boldsymbol{C}:\boldsymbol{R}]=2$。

这个例子中，$\boldsymbol{C}=\boldsymbol{R}(i)$是$\boldsymbol{R}$的单代数扩域。一般地，我们有

定理1 单代数扩域是有限扩域。

证明：设$E=F(\alpha)$，α的极小多项式设为n次多项式$p(x)$，则由上节定理5，E的元素可唯一地表为：$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$。因而，1，$\alpha$，…，$\alpha^{n-1}$构成$E$的一组基，

$[E:F]=n$。

证毕

定理 2 单超越扩域是无限扩域。

证明：设 α 是域 F 的超越元。假如 $E=F(\alpha)$ 是 F 的 n 次扩域，E 中任意 $n+1$ 个元素将线性相关，特别是 $1,\alpha,\alpha^2,\cdots,\alpha^n$ 线性相关，即存在不全为零的元素 $a_0,a_1,a_2,\cdots,a_n\in F$，满足

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0。$$

说明 α 是多项式

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$$

的根，$f(x)\neq 0(x)$，故 α 是 F 的代数元，推出矛盾。所以 $[F(\alpha):F]=\infty$。

证毕

三、代数扩域

定义 2 设 E 是域 F 的扩域，如果 E 的每个元素都是 F 的代数元，则 E 称为 F 的代数扩域。

定理 3 域 F 的有限扩域 E 是 F 的代数扩域。

证明：设 $[E:F]=n$，则对于 $\alpha\in E$，$1,\alpha,\cdots,\alpha^n$ 线性相关（元素个数>维数 n），则在 F 中存在不全为零的元素 $a_0,a_1,\cdots,a_n$，适合

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0,$$

因而 α 是 F 上非零多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$ 的根。即 α 是 F 的代数元，E 是 F 的代数扩域。

证毕

推论 1 单代数扩域是代数扩域。

四、扩域的扩域

域 F 的单代数扩域 $F(\alpha)$，作为一个域也可以有单代数扩域 $F(\alpha)(\beta)$，记为 $F(\alpha,\beta)$。一般地，$F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$ 的单代数扩域 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n)$ 记为 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_n)$。它显然包含 F 和 $\alpha_1,\alpha_2,\cdots,\alpha_{n-1}$，$\alpha_n$。另外，任意包含 F 和 α_1，α_2，…，α_{n-1}，α_n 的域都一定包含 $F(\alpha_1)$，$F(\alpha_1)(\alpha_2)$，…，$F(\alpha_1)(\alpha_2)\cdots(\alpha_{n-1})(\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_n)$，所以 $F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_n)$ 是包含 F 和 α_1，α_2，…，α_{n-1}，α_n 的最小域，且与这 n 个元素的次序无关。

那末，$F(\alpha_1,\cdots,\alpha_n)$ 是不是 F 的代数扩域呢？这个问题可以从以下定理得到答案。

定理 4 设 K 是 F 的 n 次扩域，E 是 K 的 m 次扩域，则 E 是 F 的 mn 次扩域。

证明： 设 u_1，…，u_n 是 K 作为 F 上的 n 维向量空间的一组基，v_1，…，v_m 是 E 作为 K 上的 m 维向量空间的一组基。任取 $\alpha\in E$，则

$$\alpha=\sum_{j=1}^{m}\lambda_j v_j,\quad \lambda_j\in K,$$

同样，$\lambda_j=\sum_{i=1}^{n}\mu_{ij}u_i$，$j=1$，…，$m$，其中 $\mu_{ij}\in F$。所以，

$\alpha=\sum_{i=1}^{n}\sum_{j=1}^{m}\mu_{ij}u_i v_j$，可由 $u_1v_1,\cdots,u_1v_m,\cdots,u_nv_1,\cdots,u_nv_m$ 线性表示。

下面证明 $u_1v_1,\cdots,u_1v_m,\cdots,u_nv_1$，…，$u_nv_m$ 线性无关。设有等式

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\mu_{ij}u_iv_j=0,\ 其中\mu_{ij}\in \boldsymbol{F},$$

由于u_1, …, u_n 在 K 上的向量空间 K 中线性无关，故对于 $i=1$, …, n, 有 $\sum_{j=1}^{m}\mu_{ij}v_j=0$。又因 v_1, …, v_m 在 F 上的向量空间 K 中线性无关，故对于 $i=1$, …, n, $j=1$, …, m, 有 $\mu_{ij}=0$。所以，u_1v_1, …, u_1v_m, …, u_nv_1, …, u_nv_m 是 $\boldsymbol{E}$ 在 $\boldsymbol{F}$ 上的一组基，$[E,F]=mn$。

证毕

定理 4 在域论中是重要定理之一，它起着与群论中的拉格朗日定理类似的作用。

推论 2 设 E 是 F 的 n 次扩域，K 是 E 和 F 的中间扩域，则 $[K:F]$ 是 n 的因子。

证明：由于 $[E:F]=[E:K][K:F]$，故 $[K:F]|n$。

例 2 求证：不存在 $\boldsymbol{Q}$ 的扩域 K 严格地在 $\boldsymbol{Q}$ 和 $\boldsymbol{Q}(\sqrt[7]{2})$ 之间。

证明：设有上边所说的 K，则

$$[\boldsymbol{Q}(\sqrt[7]{2}):K][K:\boldsymbol{Q}]=[\boldsymbol{Q}(\sqrt[7]{2}):\boldsymbol{Q}].$$

$\sqrt[7]{2}$ 的极小多项式是 x^7-2，故上式右端 $=7$。7 是素数，所以左端两因子必有一个是 1。因而或者 $K=\boldsymbol{Q}$，或者 $K=\boldsymbol{Q}(\sqrt[7]{2})$。

例 3 求 $[\boldsymbol{Q}(\sqrt{2},i):\boldsymbol{Q}]=?$

解：$[\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}]=2$。$x^2+1$ 是 i 在 $\boldsymbol{Q}(\sqrt{2})$ 上的极小多项式，所以 $[\boldsymbol{Q}(\sqrt{2},i):\boldsymbol{Q}(\sqrt{2})]=2$。

$[\boldsymbol{Q}(\sqrt{2},i):\boldsymbol{Q}]=[\boldsymbol{Q}(\sqrt{2},i):\boldsymbol{Q}(\sqrt{2})][\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}]=4$.

例 4 求证：$\boldsymbol{R}$ 是 $\boldsymbol{Q}$ 的无限扩域。

证明：实数$\sqrt[n]{2}$在$\mathbf{Q}$上的极小多项式是x^n-2。$[\mathbf{R}:\mathbf{Q}]=[\mathbf{R}:\mathbf{Q}(\sqrt[n]{2})][\mathbf{Q}(\sqrt[n]{2}):\mathbf{Q}]=[\mathbf{R}:\mathbf{Q}(\sqrt[n]{2})]\cdot n$，即任意自然数$n$都整除$[\mathbf{R}:\mathbf{Q}]$。所以，$[\mathbf{R}:\mathbf{Q}]=\infty$。

推论 3 设F_{i+1}是域F_i的有限扩域，$i=1,\cdots,n-1$，则F_n是F_1的有限扩域，且

$$[F_n:F_1]=[F_n:F_{n-1}][F_{n-1}:F_{n-2}]\cdots[F_2:F_1].$$

证明：连续利用定理 4。

推论 4 设E是域F的扩域，$\alpha\in E$是F的代数元，$\beta\in F(\alpha)$，则β在F上的次数是α在F上的次数的因子。

证明：显然$F(\beta)$是$F(\alpha)$的子域。因而

$$[F(\alpha):F]=[F(\alpha):F(\beta)][F(\beta):F].$$

$[F(\alpha):F]$即α在F上的次数，$[F(\beta):F]$是β在F上的次数，所以结论成立。

证毕

例 5 求证：x^3-2在$\mathbf{Q}(\sqrt{2})$中不存在根。

证明：假设$\alpha\in\mathbf{Q}(\sqrt{2})$，$\alpha$是$x^3-2$的根，$x^3-2$是$\mathbf{Q}$上的既约多项式，所以$\alpha$是$\mathbf{Q}$上的 3 次元，$3\nmid 2$，与推论 4 矛盾。

例 6 找出$\mathbf{Q}(\sqrt{2},i)$作为$\mathbf{Q}$上的向量空间的一组基。

解：根据定理 4 的证明，只要找出$\mathbf{Q}(\sqrt{2},i)$在$\mathbf{Q}(\sqrt{2})$上的一组基和$\mathbf{Q}(\sqrt{2})$在$\mathbf{Q}$上的一组基，分别相乘即得$\mathbf{Q}(\sqrt{2},i)$在$\mathbf{Q}$上的基。

$1,\sqrt{2}$是$\mathbf{Q}(\sqrt{2})$在$\mathbf{Q}$上的一组基；

$1,i$是$\mathbf{Q}(\sqrt{2},i)$在$\mathbf{Q}(\sqrt{2})$上的一组基。

所以，$1,\sqrt{2},i,\sqrt{2}i$是我们要求的基。

例 7 求证：$\mathbf{Q}(\sqrt{2},i)=\mathbf{Q}(\sqrt{2}+i)$。

证明：$\sqrt{2}+i\in \mathbf{Q}(\sqrt{2},i)$，所以 $\mathbf{Q}(\sqrt{2}+i)$ 是 $\mathbf{Q}(\sqrt{2},i)$的子域。即

$$[\mathbf{Q}(\sqrt{2},i):\mathbf{Q}]$$
$$=[\mathbf{Q}(\sqrt{2},i):\mathbf{Q}(\sqrt{2}+i)][\mathbf{Q}(\sqrt{2}+i):\mathbf{Q}].$$

由例 3，$[\mathbf{Q}(\sqrt{2},i):\mathbf{Q}]=4$。又由 §5·3 例 1，$\sqrt{2}+i$ 是 $\mathbf{Q}$ 上的 4 次元，即$[\mathbf{Q}(\sqrt{2}+i):\mathbf{Q}]=4$。所以$[\mathbf{Q}(\sqrt{2},i):\mathbf{Q}(\sqrt{2}+i)]=1$，即 $\mathbf{Q}(\sqrt{2},i)=\mathbf{Q}(\sqrt{2}+i)$。

现在回到定理 4 前面提出的问题上来。

定理 5 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是域 F 的代数元，则 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是 F 的有限扩域，因而是代数扩域。反之，F 的任意有限扩域 E 形如 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。

证明：当 $n=1$ 时，由推论 1 证实。

设当 $n-1$ 时定理正确，则当 n 时，

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_n)$$
$$=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n),$$

因而，

$$[E:F]=[E:F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})][F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1}):F].$$

由归纳假定，右端为自然数。E 是 F 的有限扩域。反之，设 E 是 F 的有限扩域，α_1，$\alpha_2,\cdots,\alpha_n$ 是 E 在 F 上的基，那末显然 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)\subseteq E$。任取 $\alpha\in E$，则 $\alpha=\sum_{i=1}^{n}\lambda_i\alpha_i\in F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，即 $E\subseteq F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$。

证毕

***例 8** 设域 F 的特征$\neq 2$，E 是 F 的 4 次扩域。求证：存在满足条件 $F\subset K\subset E$ 的 F 的二次扩域 K 的充要条件是：$E=F(\alpha)$且 α 在 F 上的极小多项式是 x^4+ax^2+b。

证明：充分性．设α在F上的极小多项式是x^4+ax^2+b，则$\alpha^2\overline{\in}F$（否则α是$x^2-\alpha^2$的根），$\alpha\overline{\in}F(\alpha^2)$（否则$\alpha=k\alpha^2+l$，$k,l\in F$，$\alpha$是多项式$kx^2-x+l$的根），因而$[F(\alpha^2):F]\neq1$，$[F(\alpha):F(\alpha^2)]\neq1$．但$[F(\alpha):F]=[F(\alpha):F(\alpha^2)][F(\alpha^2):F]=4$，故$[F(\alpha^2):F]=2$．令$K=F(\alpha^2)$，则$K$是$F$的二次扩域，适合$F\subset K\subset E$．

必要性．设K是适合$F\subset K\subset E$的F的二次扩域．取K在F上的一组基$\{1,t\}$，设$t^2=a_1t+a_2\in K(a_1,\ a_2\in F)$，$a_3=(2\cdot1)^{-1}a_1$（1为$F$的单位元，由于$F$特征$\neq2$，故$2\cdot1\neq0$），$a_4=a_2+a_3^2\in F$，$\beta=t-a_3\in K\backslash F$．易见$\beta^2=a_4$．同法可在$E\backslash K$中找到$\gamma$，$\gamma^2=b_1=a_5\beta+a_6\in K$．如果$b_1\overline{\in}F(a_5\neq0)$，则$F(\gamma^2)=F(b_1)=K$，$K(\gamma)=E$，$F(\gamma)=E$．而易见$\gamma$是多项式$f(x)=x^4+(-2a_6)x^2+(a_6^2-a_5^2a_4)$的根．由于$E=F(\gamma)$是四次扩域，可知$f(x)$是$\gamma$在$F$上的极小多项式．取$\alpha=\gamma$，$f(x)$的相应系数为$a$，$b$，即为所求．如果$b_1\in F$，即$a_5=0$，可取$\alpha=\beta+\gamma\in E\backslash K$．易见$\beta=(2\alpha)^{-1}(\alpha^2+a_4-a_6)\in F(\alpha)$，同理$\gamma\in F(\alpha)$．故$E=F(\beta,\gamma)=F(\alpha)$．可以算出，$\alpha$是多项式

$$g(x)=x^4+[2(a_4-a_6)-4a_4]x^2+(a_4-a_6)^2$$

的根．由于$E=F(\alpha)$为四次扩域，故$g(x)$是α在F上的极小多项式．令$g(x)$相应系数为a，b，即为所求．

定理6 设α,β是域F上的代数元，则$\alpha\pm\beta$，$\alpha\beta,\alpha\beta^{-1}$（$\beta\neq0$）是$F$上的代数元．因而$F$的任意扩域$E$中，$F$的全体代数元作成$E$的子域．

证明： $F(\alpha,\beta)$是F的代数扩域，$\alpha,\beta\in F(\alpha,\beta)$，因而$\alpha\pm\beta$，$\alpha\beta,\alpha\beta^{-1}(\beta\neq 0)$都属于$F(\alpha,\beta)$，即为$F$的代数元。

证毕

前面我们看到，有限扩域是代数扩域，那末，代数扩域是不是有限扩域呢？不一定。

定理 7 $\mathbf{Q}$在$\mathbf{R}$中的全体代数元作成的域A是$\mathbf{Q}$的无限扩域。

证明： 对于任意的n，$\sqrt[n]{2}$显然是$\mathbf{Q}$上的n次元。$[A:\mathbf{Q}]=[A:\mathbf{Q}(\sqrt[n]{2})][\mathbf{Q}(\sqrt[n]{2}):\mathbf{Q}]=[A:\mathbf{Q}(\sqrt[n]{2})]\cdot n$。$n$可以取任意正整数，所以，$A$是$\mathbf{Q}$的无限扩域。

证毕

这样看来，代数扩域是比有限扩域更广泛的一类扩域。有限扩域具有传递性（定理 4），有趣的是，代数扩域也具有这种性质：

定理 8 设E是K的代数扩域，K是F的代数扩域，则E是F的代数扩域。

证明： 任取$u\in E$，则u是一个多项式

$$f(x)=a_0+a_1x+\cdots+a_mx^m\in K[x]$$

的根，$a_0,a_1,\cdots,a_m\in K$，故是F上的代数元，由定理 5，$F(a_0,a_1,\cdots,a_m)$是F的有限扩域，同理，$F(a_0,a_1,\cdots,a_m)(u)$是F的有限扩域因而是代数扩域，u是F的代数元。由于u的任意性，E是F的代数扩域。

证毕

习 题 5·4

1. 试求：$[Q(\sqrt{2}):Q]$；$[Q(\sqrt{2},\sqrt{3}):Q(\sqrt{2})]$；$[Q(\sqrt{2},\sqrt{3},\sqrt{5}):Q]$. 并给出各扩域的一组基。

2. 求证：多项式 x^2-2 在 $Q(\sqrt[3]{2})$ 上既约。

3. 求证：$Q(\sqrt{2}+\sqrt{3})=Q(\sqrt{2},\sqrt{3})$。

4. 设 E，F 是域 K 的子域，$F\subseteq E$，且 $[K:E]=[K:F]$，求证：$E=F$。

5. 设 E 是 F 的有限扩域，$[E:F]=p$（素数）。求证：E 是 F 的单扩域。

6. 设 E 是域 F 的有限扩域，$p(x)$ 是 F 上高于一次的既约多项式，其次数与 $[E:F]$ 互素，求证：$p(x)$ 在 E 中无根。

7. 设 E 是域 F 的代数扩域，$f(x)$ 与 $g(x)$ 在 $F[x]$ 中互素，求证也在 $E[x]$ 中互素.

§5·5 分 裂 域

本节介绍多项式的分裂域的概念以及分裂域的存在性及唯一性定理。

一、分裂域的概念

考虑有理数域 Q 上的多项式 $f(x)=x^2-2$。显然 $f(x)$ 在 $Q[x]$ 中不能完全分解，而在 Q 的扩域 $Q(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in Q\}$ 上的多项式环中能分解为一次因子之积：$f(x)=(x+\sqrt{2})(x-\sqrt{2})$。易见，$f(x)$ 在 $Q(\sqrt{2})$ 的任何真子域上的多项式环中不能分解为一次因子之积。$Q(\sqrt{2})$ 对于 $f(x)$

来说是一种特殊的域。

定义1 设$f(x)$是域F上的多项式，如果$f(x)$在F的扩域E上的多项式环中可以分解为一次因子的乘积：

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

但在E的任一真子域上的多项式环中不能这样分解，则称E是$f(x)$在F上的分裂域。

根据因式定理，$x-\alpha|f(x)$等价于α是$f(x)$的根，所以，F上的多项式$f(x)$的分裂域就是包含其全部根的最小扩域，即

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

其中α_1，$\alpha_2,\cdots,\alpha_n$是$f(x)$的全部根。

所以，域F的任一多项式的分裂域总是F的有限扩域，因而是代数扩域。

同一多项式看作不同域上的多项式时，其分裂域可能不同，如$f(x)=x^2-2$看作$\boldsymbol{R}[x]$中的多项式时，其分裂域是$\boldsymbol{R}$，而看作$\boldsymbol{Q}[x]$中的多项式时，其分裂域是$\boldsymbol{Q}(\sqrt{2})$。

另外值得注意的是，不能把分裂域等同为包含全部根的扩域。例如$\boldsymbol{Q}[x]$中x^2-2的全部根包含在$\boldsymbol{R}$中，$\boldsymbol{R}$不是x^2-2的分裂域，因为$\boldsymbol{R}$不是包含全部根的最小扩域，而$\boldsymbol{Q}(\sqrt{2})$才是其分裂域。

二、分裂域的存在性

$F[x]$中任一多项式$f(x)$是否总有分裂域呢？怎样找出$f(x)$的分裂域呢？先用一个例子说明。

例1 设$F=\boldsymbol{Q}$，$f(x)=x^4-x^2-2$，试求$f(x)$的分裂域。

解：首先，在$\boldsymbol{Q}[x]$中将$f(x)$分解为既约多项式的乘积：

$f(x)=(x^2+1)(x^2-2)$(x^2+1 和 x^2-2 显然是 $\mathbf{Q}[x]$ 中的既约多项式)。根据§5·3定理7，存在 $\mathbf{Q}$ 的单代数扩域 $E=\mathbf{Q}(\alpha)=\{a\alpha+b\mid a,b\in\mathbf{Q}\}\cong\mathbf{Q}[x]/\langle x^2-2\rangle$，包含 x^2-2 的一个根。在 E 上 x^2+1 仍是既约的，这是因为 x^2+1 在 E 中无根。事实上，假如 $a\alpha+b\in E$ 是 x^2+1 的根，则 $(a\alpha+b)^2=a^2\alpha^2+2ab\alpha+b^2=-1$。但 α 是 x^2-2 的根，故 $\alpha^2=2$，$(a\alpha+b)^2=2ab\alpha+2a^2+b^2$，即 $2ab\alpha+2a^2+b^2=-1$，由表示的唯一性，得 $2a^2+b^2=-1$。a，b 是有理数，上式不能成立。所以，x^2+1 在 E 上是既约多项式。再一次利用§5·3定理7，构造 E 的单代数扩域 $K\cong E[x]/\langle x^2+1\rangle$，包含 x^2+1 的一个根，因而包含所有的根。K 是 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域，且 $[K:E][E:\mathbf{Q}]=2\cdot2=4$。

定理1 设 $f(x)\in F[x]$，则存在 $f(x)$ 在 F 上的分裂域。

证明：对 $f(x)$ 的次数施行数学归纳法。

当 $n=1$ 时，F 即 $f(x)$ 的分裂域。

假定定理对低于 n 次的多项式成立。设 $f(x)$ 是 n 次多项式，取 $f(x)$ 的既约因子 $p(x)$[注]（如果 $f(x)$ 本身就是既约的，则迳取 $p(x)=a_n^{-1}f(x)$，其中 a_n 是 $f(x)$ 的首项系数），由§5·3定理7，存在 F 的单代数扩域 $E=F(\alpha)\cong F[x]/\langle p(x)\rangle$，包含 E 的一个根 α。根据因式定理，在 $E[x]$ 中，$f(x)=(x-\alpha)g(x)$，其中 $g(x)$ 是 $n-1$ 次多项式。由归纳假定，$g(x)$ 在 E 上存在分裂域 $E(\alpha_2,\cdots,\alpha_n)=F(\alpha,\alpha_2,\cdots,\alpha_n)$，其中 $\alpha_2,\cdots,\alpha_n$ 是 $g(x)$ 的根，即得 $f(x)$ 在 F 上的分裂域。

证毕

注　本节提到的既约多项式，一律设首项系数为1。

例2 设 $F=\mathbf{Z}_2$，$f(x)=[1]x^4+[1]x^3+[1]x^2+[1]$，求 $f(x)$ 在 $\mathbf{Z}_2$ 上的分裂域。

解：$\mathbf{Z}_2$ 中只有两个元素：$[0]$ 和 $[1]$，本题以下简记为 0，1注。$f(0)=1\neq 0$，$f(1)=1+1+1+1=0$。因而 1 是根，$x-1\mid f(x)$。显然 $f(x)=(x-1)(x^3+x+1)$。设 $g(x)=x^3+x+1$，$f(x)$ 的分裂域即 $g(x)$ 的分裂域。$g(0)=1\neq 0$，$g(1)=1+1+1=1\neq 0$，故 $g(x)$ 在 $\mathbf{Z}_2$ 无根，是 $\mathbf{Z}_2[x]$ 中的既约多项式。存在 $\mathbf{Z}_2$ 的扩域 $\mathbf{Z}_2(\alpha)\cong\mathbf{Z}_2[x]/\langle g(x)\rangle$，包含 $g(x)$ 的根 α。在 $\mathbf{Z}_2(\alpha)$ 上，$g(x)$ 可以分解为

$$g(x)=(x-\alpha)(x^2+ax+b),$$

即 $\quad x^3+x+1=x^3+(a-\alpha)x^2+(b-a\alpha)x-b\alpha$。

所以

$$\begin{cases}a-\alpha=0,\\ b-a\alpha=1,\\ -b\alpha=1.\end{cases}$$

得 $a=\alpha$，$b=\alpha^2+1$。

$\mathbf{Z}_2(\alpha)$ 是 $\mathbf{Z}_2$ 的三次扩域，其元素形如

$$a_1+a_2\alpha+a_3\alpha^2,$$

其中 a_1，a_2，$a_3\in F$。

因而 $\mathbf{Z}_2(\alpha)$ 共有 8 个元素：

$$0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2.$$

代入 $g(x)$，可见 α^2 和 α^3 是根。因而 $f(x)$ 在 $F(\alpha)$ 上可以分解为：

$$f(x)=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3).$$

注 本书以下对 $\mathbf{Z}_n$ 的元素 $[k]$ 简记为 k，注意防止与整数 k 混淆。

例 3 写出 $\mathbf{Q}$ 上的多项式 $f(x)=x^5-1$ 的分裂域。

解：$f(x)=(x-1)(x^4+x^3+x^2+x+1)$ 的分裂域显然是多项式 $g(x)=x^4+x^3+x^2+x+1$ 的分裂域。$g(x)$是 $\mathbf{Q}$ 上的既约多项式（见本丛书《多项式代数》§4·3）。所以存在 $\mathbf{Q}$ 的扩域 $E=\mathbf{Q}(\alpha)\cong\mathbf{Q}[x]/\langle g(x)\rangle$包含 $g(x)$的根 α。显然 $\alpha^5=1,\alpha\neq1$。α 在 E 的非零元乘群$\langle E^*,\cdot\rangle$中是 5 阶元，即 1，α，α^2，α^3，α^4 是 E 中互不相同的元素，它们都是 $f(x)$的根，且是全部根：

$$x^5-1=(x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4).$$

因此，$E=\mathbf{Q}(\alpha)$是 $f(x)$的分裂域，$[E:\mathbf{Q}]=4$。

三、分裂域的唯一性

一个多项式可能由于方法的不同得到不同的分裂域，但从同构的观点出发，实质上是一样的。为了证明这一点，引进一个新的概念。

定义 2 设 E 和 $\bar{E}$ 分别是域 F 和 $\bar{F}$ 的扩域，$F\cong\bar{F}$，$E\cong\bar{E}$，且 F 中的元素在这两种同构映射下象对应相等，则称第二个同构是第一个同构的扩张。

显然，域的等价（§5·3 定义 3）是子域的恒等自同构的扩张。

设 $f(x)\in F[x]$，$F\cong\bar{F}$，把 $f(x)$的系数换成 $\bar{F}$ 中的对应元素，得到 $\bar{F}$ 上的多项式，记为 $\bar{f}(x)$。

定理 2 设域 $F\cong\bar{F}$，$p(x)$为 $F[x]$ 中的既约多项式，则 $\bar{p}(x)$为 $\bar{F}[x]$中的既约多项式。设 $F(\alpha)$ 是 F 的扩域，$p(\alpha)=0$，$\bar{F}(\bar{\alpha})$ 是 $\bar{F}$ 的扩域，$\bar{p}(\bar{\alpha})=0$，则 $F(\alpha)\cong\bar{F}(\bar{\alpha})$，它是 $F\cong\bar{F}$ 的扩张，并将 α 映为 $\bar{\alpha}$。

证明：假若 $\bar{p}(x)$有真因子 $\bar{p}_1(x)$，则 $\bar{p}_1(x)$ 在 $F[x]$ 中

对应的多项式 $p_1(x)$ 是 $p(x)$ 的真因子，所以 $\bar{p}(x)$ 是 $\bar{F}[x]$ 中的既约多项式。

设 $p(x)$ 的次数为 n，则 $\bar{p}(x)$ 的次数也是 n。$F(\alpha)$ 的元素可唯一地表为 $a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$，$\bar{F}(\bar{\alpha})$ 的元素可唯一地表为 $\bar{a}_0+\bar{a}_1\bar{\alpha}+\cdots+\bar{a}_{n-1}\bar{\alpha}^{n-1}$　作映射

$$\varphi(a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1})=\bar{a}_0+\bar{a}_1\bar{\alpha}+\cdots+\bar{a}_{n-1}\bar{\alpha}^{n-1},$$

其中 $\bar{a}_i\in\bar{F}$ 是 $a_i\in F$ 的同构象。φ 是一一映射。又因 $F(\alpha)$ 和 $\bar{F}(\bar{\alpha})$ 的元素的运算，显然除了横线之外，是完全一样的，因而 φ 是 $F(\alpha)$ 到 $\bar{F}(\bar{\alpha})$ 的同构。易见，对于 $a\in F$，$\varphi(a)=\bar{a}$，且 $\varphi(\alpha)=\varphi(0+1\alpha)=\bar{0}+\bar{1}\bar{\alpha}=\bar{\alpha}$。

证毕

定理 3　如果域 $F\cong\bar{F}$，$f(x)\in F[x]$，则 $f(x)$ 的分裂域与 $\bar{f}(x)$ 的分裂域同构，它是 F 到 $\bar{F}$ 同构的扩张。

证明：如果 $f(x)$ 已在 $F[x]$ 中分解为一次因子之积，则 $\bar{f}(x)$ 也在 $\bar{F}$ 上分解为一次因子之积。这时，定理显然成立。

如果 $f(x)$ 在 $F[x]$ 中有高于一次的既约因子 $p(x)$，则 $\bar{f}(x)$ 有既约因子 $\bar{p}(x)$。作单扩域 $F(\alpha)$，使 $p(\alpha)=0$，作单扩域 $\bar{F}(\bar{\alpha})$，使 $\bar{p}(\bar{\alpha})=0$。由定理 2，$F(\alpha)\cong\bar{F}(\bar{\alpha})$，且为 $F\cong\bar{F}$ 的扩张。

在 $F(\alpha)$ 上，$f(x)$ 可以分解为

$$f(x)=(x-\alpha)g(x).$$

在 $\bar{F}(\bar{\alpha})$ 上，$\bar{f}(x)$ 可以分解为

$$\bar{f}(x)=(x-\bar{\alpha})\bar{g}(x).$$

如果这时 $g(x)$ 已分解为一次因子之积，则定理得证，否则，在 $F(\alpha)$ 和 $\bar{F}(\bar{\alpha})$ 上重新讨论 $g(x)$ 和 $\bar{g}(x)$。由于次数的限制，经有限次，可以得到 $f(x)$ 和 $\bar{f}(x)$ 的分裂域 E 和 $\bar{E}$。由于每

一步都是 $F\cong\bar{F}$ 的扩张，所以 $E\cong\bar{E}$，且是 $F\cong\bar{F}$ 的扩张。

证毕

定理 4 域 F 上的多项式 $f(x)$ 任意两个分裂域等价。

证明：在定理 3 中，取 $\bar{F}=F$，则 $f(x)=\bar{f}(x)$，两个分裂域是 F 中恒等同构的扩张，即相互等价。

证毕

综合定理 1 和定理 4，可知域上的任意多项式的分裂域总是存在的，且除等价外是唯一的。

习 题 5·5

1．设 $f(x)=x^2+ax+b, a, b\in F$，如果 $f(x)$ 在 $F[x]$ 中可约，求证 F 是 $f(x)$ 的分裂域．如果 $f(x)$ 在 $F[x]$ 中既约，则 $f(x)$ 的分裂域是 F 的单代数扩域．

2．x^3-5 在 $\mathbf{Q}$ 上分裂域是 $\mathbf{Q}$ 的几次扩域？

*3．求证：n 次多项式在域 F 上的分裂域作为 F 的扩域的次数至多是 $n!$．

4．设 θ 是 n 次原根，求证：$\mathbf{Q}(\theta)$ 是多项式 x^n-1 在 $\mathbf{Q}$ 上的分裂域．

*5．设 $f(x)=x^p-1$，p 为素数，E 为 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域，求证：$[E:\mathbf{Q}]=p-1$．

6．设 $f(x)=(x^2-2)(x^2-3)$，试求 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域，并求它关于 $\mathbf{Q}$ 的扩域次数．

§5·6 可分扩域

有时，域的若干次单代数扩域 $F(\alpha_1)(\alpha_2)\cdots(\alpha_n)=F(\alpha_1,$

$\alpha_2,\cdots,\alpha_n$)可以用一个单代数扩域代替，即 $F(\alpha)=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.（如§5·4 例 7）

这样，就使域的扩张得到很大的简化. 现在就来讨论这个问题，先要讲一些预备知识，引进多项式的导数、多项式的重根以及可分性等概念。

一、重根

定义 1 域 F 上的多项式在其分裂域上如果所有一次因子彼此不同，则称 $f(x)$ 无重根. 否则称为有重根。

设在域 F 上的多项式 $f(x)$ 的分裂域上，有

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

合并相同的因子（如果有的话），可得

$$f(x)=a(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_r)^{k_r},$$

其中 $k_1+k_2+\cdots+k_r=n$，α_1，$\alpha_2,\cdots,\alpha_r$ 互不相同. 这时称 α_1 是 k_1 重根，α_2 是 k_2 重根，$\cdots$，α_r 是 k_r 重根。

一般地，如果 $(x-\alpha)^k\mid f(x)$，但 $(x-\alpha)^{k+1}\nmid f(x)$，则称 α 是 $f(x)$ 的 k 重根. 若 $k=1$，则称 α 为单根. 如 2 是 $f(x)=(x-2)^2(x-3)(x+1)$ 的二重根，而 3 和 -1 都是单根。

为了判断有无重根，引进导数的概念。

定义 2 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$，多项式

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1\in F[x] \quad (1)$$

称为 $f(x)$ 的导数。

注意：微分学中导数是借助实数域所特有的连续性引入的，在一般的域中无法采用那种方法，这里仅形式地定义，不

过对于多项式，法则是一致的。

定理1 $(f(x)+g(x))'=f'(x)+g'(x)$； (2)

$$(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)；\tag{3}$$

$$(f^m(x))'=mf^{m-1}(x)f'(x).\tag{4}$$

证明留给读者。

定理2 $f(x)$无重根的充要条件是$f(x)$与$f'(x)$互素。注

证明：设$f(x)$有k重根α，即

$$f(x)=(x-\alpha)^k g(x),(g(\alpha)\neq 0)$$

则由定理1，

$$f'(x)=(x-\alpha)^k g'(x)+k(x-\alpha)^{k-1}g(x)$$
$$=(x-\alpha)^{k-1}[(x-\alpha)g'(x)+kg(x)].$$

由于$k-1>0$，$x-\alpha$是$f(x)$与$f'(x)$的公因式，故$f(x)$与$f'(x)$不互素。

反之，如果$f(x)$无重根，在$f(x)$的分裂域中有$f(x)=a_0(x-\alpha_1)\cdots(x-\alpha_n)$，其中$\alpha_1,\cdots,\alpha_n$互不相同，$a_0\neq 0$。

$f'(x)=a_0(x-\alpha_2)\cdots(x-\alpha_n)+\cdots+a_0(x-\alpha_1)\cdots(x-\alpha_{n-1})$。显然，$f'(\alpha_i)\neq 0, i=1,\cdots,n$，故$x-\alpha_i\nmid f'(x)$，$f$与$f'$互素。

证毕

推论1 如果$p(x)$是$F[x]$中的既约多项式，且在分裂域中有重根，则$p'(x)=0(x)$。

证明：由于$p(x)$有重根，故$p(x)$与$p'(x)$不互素。设$d(x)\in(p(x),p'(x))$，则$d(x)$不是$F[x]$中的可逆元，$p(x)$是既约的，因而$d(x)$与$p(x)$相伴，其次数与$p(x)$相同，$d(x)$

注 $f(x)$有无重根是指在其分裂域上而言的，下同。

$|p'(x)$，如果 $p'(x)\neq 0(x)$，则次数应比 $p(x)$ 低一次，推出矛盾。所以 $p'(x)=0(x)$。

证毕

推论 2 若 F 的特征为∞，则 F 上的既约多项式 $p(x)$ 在分裂域中无重根。

证明：由推论 1，$p(x)$ 若有重根，则 $p'(x)=0(x)$。因而由(1)式，$p(x)$ 应为零次多项式或 $0(x)$，即 $p(x)=c\in F$，与 $p(x)$ 是既约多项式矛盾（既约多项式不是 $F[x]$ 中的可逆元或零元）。所以 $p(x)$ 无重根。

证毕

推论 3 若 F 的特征为 p，则 F 上的既约多项式 $p(x)$ 在其分裂域中有重根的充要条件是 $p(x)$ 为 x^p 的多项式，即 $p(x)=q(x^p)$，其中 $q(x)\in F[x]$。

证明：如果既约多项式

$$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$$

有重根，由推论 1，

$$0(x)=p'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1.$$

所以，每个系数都应等于 0，即

$$ia_i=0,\quad i=n,\cdots,1. \tag{5}$$

如果 $p|i$，则不论 a_i 是什么元素，都有(5)式成立，但当 $p\nmid i$ 时，就必须 $a_i=0$。于是

$$f(x)=b_mx^{pm}+\cdots+b_1x^p+b_0,$$

取 $g(x)=b_mx^m+\cdots+b_1x+b_0$，则 $f(x)=g(x^p)$。

反之，如果 $f(x)=g(x^p)=b_mx^{pm}+\cdots+b_1x^p+b_0$，则 $f'(x)=pmb_mx^{pm-1}+\cdots+pb_1x^{p-1}$。其系数都是0，即 $f'(x)=0(x)$，$f(x)|f'(x)$，$f(x)$ 与 $f'(x)$ 不互素，故 $f(x)$ 有重根。

证毕

例1 $\mathbf{Z}_3[x]$ 中 $f(x)=x^3+2x+1$（即 $[1]x^3+[2]x+[1]$）有无重根？

解：$f'(x)=3x^2+2=2$（因 $3=0$），是 $\mathbf{Z}_3[x]$ 中的可逆元，所以 $f'(x)$ 与 $f(x)$ 互素，$f(x)$ 无重根。

另解：$f(x)$ 是 $\mathbf{Z}_3$ 上的既约多项式（$f(0)=f(1)=f(2)=1\neq 0$，故 $f(x)$ 无一次因子），且不是 x^3 的多项式，由推论 3，它无重根（$\mathbf{Z}_3$ 的特征是 3）。

在特征是∞的域上，既约多项式（在其分裂域中）总无重根；在特征有限的域上，既约多项式（在其分裂域中）可以有重根，下面让我们看一个例子。

例2 设 $F=\mathbf{Z}_p(x)$（$\mathbf{Z}_p$ 的有理分式域，其元素形如 $\dfrac{f_1(x)}{f_2(x)}$，$f_2(x)\neq 0(x)$，$f_1(x)$，$f_2(x)\in\mathbf{Z}_p[x]$），求证：F 的特征为 p，且 F 上的多项式 $f(y)=y^p-x$ 是 $F[y]$ 中的既约多项式，但在其分裂域中有重根。

解：$\mathbf{Z}_p$ 是 $\mathbf{Z}_p(x)$ 的子域，且非零元 $[1]$ 在 $\mathbf{Z}_p$ 中的阶为 p，在 $\mathbf{Z}_p(x)$ 中的阶也是 p，所以 F 的特征也是 p。x 是 F 中的元素，x 不是 F 中任何元素的 p 次幂。事实上，如果

$$x=\left(\frac{a_0+a_1x+\cdots+a_nx^n}{b_0+b_1x+\cdots+b_mx^m}\right)^p,$$

则 $x(b_0+b_1x+\cdots+b_mx^m)^p=(a_0+a_1x+\cdots+a_nx^n)^p$，

由 §5·1 例 2，有

$$x(b_0^p+b_1^px^p+\cdots+b_m^px^{pm})=a_0^p+a_1^px^p+\cdots+a_n^px^{pn},$$

或 $a_0^p-b_0^px+a_1^px^p-b_1^px^{p+1}+\cdots+a_n^px^{pn}-b_m^px^{pm+1}=0(x)$，

所以，

$a_0=a_1=\cdots=a_n=b_0=b_1=\cdots=b_m=0$，与$b_0+b_1x+\cdots+b_mx^m\neq 0(x)$矛盾。

把x看作固定元素，考虑F上的多项式$f(y)=y^p-x$，其中y是F上的不定元。

$f(y)$是$F[y]$中的既约多项式。事实上，假如$y^p-x=g(y)h(y)$，其中$g(y)$是首项系数为1的k次多项式（$1\leqslant k\leqslant p-1$）。设$E$是$f(y)$在$F$上的分裂域，$b\in E$是$f(y)$的一个根，则有$b^p=x$。因而$y^p-x=y^p-b^p=(y-b)^p=g(y)h(y)$。因而$g(y)=(y-b)^k=y^k-ky^{k-1}+\cdots+(-1)^{k+1}b^k$。由于$g(y)\in F[y]$，故系数$(-1)^{k+1}b^k\in F$，$b^k\in F$。$k$与$p$互素（在$\mathbf{Z}$中），故有整数$u$和$v$，使$ku+pv=1$，又因$b^p=x\in F$，故$b=(b^k)^u(b^p)^v\in F$。这就是说，$x$等于$F$的元素$b$的$p$次幂，与刚才证明的结果矛盾，故$f(y)$是$F[y]$中的既约多项式。

$f(y)$在E中有重根。事实上，$f'(y)=py^{p-1}=0(y)$，由定理1知$f(y)$在分裂域E中有重根。

二、可分性

定义3 $F[x]$中的多项式$f(x)$，如果其每个既约因子在分裂域中都没有重根，则称为可分多项式。

特征为∞的域上的任何多项式都是可分的，因为这种域上的既约多项式（在分裂域中）无重根（推论2）。

由推论3，特征为p的域上的既约多项式是可分多项式的充要条件是这个多项式形如$g(x^p)$。

定义4 域F上的所有多项式如果都是可分多项式，则称F为完全域。

因而，特征为∞的域都是完全域。特征为p的域什么时

候是完全的呢？

定理 3 特征为 p 的域 F 是完全域的充要条件为：F 的每个元素都是 F 中某元素的 p 次幂。

证明：设 $a\in F$，a 不是任意元素的 p 次幂，则 x^p-a 是既约多项式。因若不然，设 $x^p-a=g(x)h(x)$，和例 2 的证法完全相同可以推出 a 是一个元素的 p 次幂，与 a 的假设矛盾。$(x^p-a)'=px^{p-1}=0(x)$，因而 x^p-a 是一个不可分的既约多项式，F 不是完全域。

反之，设 F 不是完全域，则存在不可分的既约多项式，例如为 $f(x)$，它在其分裂域中有重根，由推论 3，$f(x)$ 形如 $a_0+a_1x^p+\cdots+a_nx^{pn}$，系数之中一定可以找到一个不能表成 F 中元素的 p 次幂。因为如果不然，设 $a_i=b_i^p$，$i=0,1,\cdots,n$，则

$$f(x)=b_0^p+b_1^px^p+\cdots+b_n^px^{pn}=(b_0+b_1x+\cdots+b_nx^n)^p$$

与 $f(x)$ 的既约性矛盾。

证毕

定义 5 设 F 是域，a 是 F 上的代数元，如果 a 在 F 上的极小多项式是可分的，则称 a 是 F 上的可分元素。F 的扩域 E 的元素如果都是 F 上的可分元素，则称 E 是 F 的可分扩域。

特征为 ∞ 的域上的所有代数元都是可分元，因而其所有代数扩域是可分扩域。

显然，一个域是完全域的充要条件是它的所有代数扩域是可分扩域。因而特征为 p 的域当且仅当其所有元素都是域中某元素的 p 次幂时，其所有代数扩域是可分扩域。

三、可分扩域的单纯性

现在回到本节一开始提出的问题。

定理 4 设 F 是无限域，α_1，$\alpha_2,\cdots,\alpha_n$ 是 F 上的代数元，$\alpha_2,\cdots,\alpha_n$ 是 F 上的可分元，则 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 是 F 的单代数扩域，即有 $\beta\in E$，使 $E=F(\beta)$。

证明：首先证明 $n=2$ 的情形。

设 α_1 的极小多项式为 $f_1(x)$，α_2 的极小多项式为 $f_2(x)$，作 $f_1(x)f_2(x)$ 的分裂域 K，设 $\alpha_1=\beta_1,\cdots,\beta_r$ 是 $f_1(x)$ 在 K 中的所有不同的根，$\alpha_2=\gamma_1,\cdots,\gamma_s$ 是 $f_2(x)$ 在 K 中的全部不同的根。选取 $c\in F$，使对所有 $i\geqslant 1$，$j\geqslant 2$，有

$$\alpha_1+c\alpha_2\neq\beta_i+c\gamma_j,$$

即 $c\neq\dfrac{\beta_i-\alpha_1}{\alpha_2-\gamma_j}$。因为 $f_2(x)$ 可分，所以 $\alpha_2-\gamma_j$ 不会等于零，又由于 F 包含无限个元素，故上述 c 的选取是可以实现的。

令 $\beta=\alpha_1+c\alpha_2$。显然 $\beta\in F(\alpha_1,\alpha_2)$，故 $F(\beta)\subseteq F(\alpha_1,\alpha_2)$。下面证明 $F(\beta)=F(\alpha_1,\alpha_2)$。

事实上，$f_2(\alpha_2)=0$，$f_1(\beta-c\alpha_2)=f_1(\alpha_1)=0$。所以，$\alpha_2$ 是 $f_2(x)$ 和 $f_1(\beta-cx)$ 的公根。这两个多项式不会有其他公根，这因为 $\gamma_2,\cdots,\gamma_s$ 都不适合 $f_1(\beta-cx)=0$：

$$\beta-c\gamma_j=\alpha_1+c(\alpha_2-\gamma_j)\neq\alpha_1+\beta_i-\alpha_1=\beta_i,$$

$(j=2,\cdots,s,\ i=1,\cdots,r)$，同时 α_2 是 $f_2(x)$ 的单根，所以 $f_2(x)$ 与 $f_1(\beta-cx)$ 只有一个公共的一次因子 $x-\alpha_2$，故 $f_2(x)$ 和 $f_1(\beta-cx)$ 的最大公因式为 $x-\alpha_2$。$f_2(x)$ 和 $f_1(\beta-cx)$ 的系数都在 $F(\beta)$ 中。故其最大公因式 $x-\alpha_2$ 的系数 $\alpha_2\in F(\beta)$。而 $\alpha_1=\beta-c\alpha_2$ 所以也属于 $F(\beta)$，因而 $F(\alpha_1,\alpha_2)\subseteq F(\beta)$，即

$F(\alpha_1,\alpha_2)=F(\beta)$.

对于$n>2$的情况，可用归纳法得到证明.

证毕

定理证明，无限域的任意有限可分扩域是一个单代数扩域，而单代数扩域的结构是十分清楚的，例如它的元素可以唯一地表为$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}$的形式.

推论 1 特征为∞的域的有限扩域都是单代数扩域.

证明：只须证明特征为∞的域是无限域. 事实上，若这种域里若只含有限个元素，则$a, 2a, \cdots$（其中a是任一非零元）是有限元素列，设$pa=qa$，则$(p-q)a=0$，即a在加群中的阶$\leqslant p-q$，所以域的特征$\neq\infty$.

证毕

例 3 试求α，使$Q(\sqrt{2},\sqrt{3})=Q(\alpha)$.

解：Q是特征为∞的域，故其有限代数扩域$Q(\sqrt{2},\sqrt{3})$是一个单代数扩域.

$\sqrt{2}$的极小多项式是x^2-2，其根为$\sqrt{2}$，$-\sqrt{2}$. $\sqrt{3}$的极小多项式是x^2-3，其根为$\sqrt{3}$，$-\sqrt{3}$. 选取$c\neq\frac{-\sqrt{2}-\sqrt{2}}{\sqrt{3}-(-\sqrt{3})}=-\frac{2\sqrt{2}}{2\sqrt{3}}=-\frac{\sqrt{2}}{\sqrt{3}}$，且$c\neq 0$. 例如可取$c=1$，令$\alpha=\sqrt{2}+1\cdot\sqrt{3}=\sqrt{2}+\sqrt{3}$，即为所求.

注意：本例所使用的方法就是定理 4 的证明中所提供的方法. 由于c的取法是无限的，所以α可有无限多种取法. 例如$\alpha=\sqrt{2}+2\sqrt{3}$，$\alpha=\sqrt{2}-\sqrt{3}$，等.

习 题 5·6

1. 判断以下多项式在其分裂域中有无重根?

(1) $x^3+2x+1\in \mathbf{Q}[x]$； (2) $x^3+2x+2\in \mathbf{Z}_3[x]$；

(3) $x^p-1\in \mathbf{Z}_p[x]$； (4) $x^p-(p-1)\in \mathbf{Z}_p[x]$；

(5) $x^p-x-a\in \mathbf{Z}_p[x]$.

2. 设 F 是不完全域，特征为 p，求证：$x^{p^n}-a$ 既约的充要条件是 a 不是 F 中任意元素的 p 次幂.

3. 设域 F 的所有扩域都是可分的，求证：F 的任意代数扩域的所有扩域也都是可分的.

4. 求元素 α，使 $\mathbf{Q}(\alpha)=\mathbf{Q}\left(\sqrt{2}\,i,\ \dfrac{-1+\sqrt{3}\,i}{2}\right)$.

5. 求元素 t，使 $\mathbf{Q}(t)=\mathbf{Q}(r,s)$，其中 r 是 x^2+x+1 的根，s 是 x^2+4 的根.

6. 证明本节定理1.

7. 设 $F[x]$ 是域 F 上的多项式环，D 是求导变换：$D(f(x))=f'(x)$. 求证：D 是 $\langle F[x],+\rangle$ 的同态变换. 并求 D 的核.

§5·7 有 限 域

有理数域、实数域等常见的域含有无限多个元素，而域 $\mathbf{Z}_2$、$\mathbf{Z}_3$、$\mathbf{Z}_5$ 等只含有限个元素. 有限域指的是元素有限多的域，它有许多独特的性质.

一、元素的个数

有限域的特征不会为 ∞，所以总是一个素数 p. 我们知道，任给一个正整数 n，总有 n 阶群（如 C_n）和 n 阶环（如 $\mathbf{Z}_n$），却不一定有 n 元域，这因为域的元素个数具有特殊的规

律。

定理1 有限域中元素个数是其特征的正整数方幂。

证明：设有限域F的特征为p，由§5·1定理8，F含有素域$F_0\cong \mathbf{Z}_p$，因而$|F_0|=p$。F是F_0的有限扩域。设$[F:F_0]=n$，则F中每个元素可唯一地表为：

$$a_1\alpha_1+a_2\alpha_2+\cdots+a_n\alpha_n,$$

其中a_1，$a_2,\cdots,a_n\in F_0$，α_1，$\alpha_2,\cdots,\alpha_n$是F在F_0上的向量空间的一组基。由于每个a_i可以独立地取F_0中p个不同的元素，同时α_1，$\alpha_2,\cdots,\alpha_n$线性无关，故F中共有p^n个不同的元素。

证毕

反之，任给素数p和一个正整数n，是否存在含有p^n个元素的有限域呢？

定理2 设F是含p个元素的域，则F上的多项式$f(x)=x^{p^n}-x$在F上的分裂域E含p^n个元素。

证明：$f'(x)=p^nx^{p^n-1}-1=-1\neq 0$，所以$f(x)$在$E$中无重根。设$f(x)$所有根的集合为$F_1$，$F_1\subseteq E$。任取$\alpha_i$，$\alpha_j\in F_1$，则$\alpha_i^{p^n}=\alpha_i$，$\alpha_j^{p^n}=\alpha_j$，

$$(\alpha_i-\alpha_j)^{p^n}=(\cdots((\alpha_i-\alpha_j)^p)^p\cdots)^p=(\cdots(\alpha_i^p-\alpha_j^p)^p\cdots)^p$$
$$=\cdots=\alpha_i^{p^n}-\alpha_j^{p^n}=\alpha_i-\alpha_j,\text{即 }\alpha_i-\alpha_j\in F_1。$$

$$\left(\frac{\alpha_i}{\alpha_j}\right)^{p^n}=\frac{\alpha_i^{p^n}}{\alpha_j^{p^n}}=\frac{\alpha_i}{\alpha_j},\ (\alpha_j\neq 0)\text{ 即 }\frac{\alpha_i}{\alpha_j}\in F_1。$$（这里$\frac{\alpha_i}{\alpha_j}$表示$\alpha_i\alpha_j^{-1}$）

所以F_1是E的子域。下面我们证明$F\subseteq F_1$。事实上，0显然适合$x^{p^n}-x=0$。若$a\neq 0$，$a\in F$，由于$\langle F^*,\cdot\rangle$的阶为$p-1$，故$a^{p-1}=1$，而$p-1|p^n-1$，故$a^{p^n-1}=1$，或$a^{p^n}=a$，

$a\in F_1$。总之，$F\subseteq F_1$。

这样，F_1是包含F和$f(x)$所有根的最小域，故为$f(x)$在F上的分裂域。令$E=F_1$，即为所求。

证毕

例1 写出含4个、8个、16个、32个元素的域。

解：$\mathbf{Z}_2$含两个元素。

x^4-x在$\mathbf{Z}_2$上的分裂域E_1含4个元素。

x^8-x在$\mathbf{Z}_2$上的分裂域E_2含8个元素。

$x^{16}-x$在$\mathbf{Z}_2$上的分裂域E_3含16个元素。

$x^{32}-x$在$\mathbf{Z}_2$上的分裂域E_4含32个元素。

例2 有没有含100个元素的域？

解：$100=2^2\cdot 5^2$不是p^n形，故没有这样的域。

定理3 两有限域F_1和F_2的元素个数如果相同，则同构。

证明：设$|F_1|=|F_2|=p^n$。由定理2，各含一个素域P_1和P_2同构于$\mathbf{Z}_p$。F_1和F_2都是P_1和P_2的多项式$x^{p^n}-x$的分裂域。由§5·5定理3，$F_1\cong F_2$。

证毕

同阶群或环不一定同构，但同样多元素作成的域却是同构的。或者说，域的性质，由其所含元素的个数唯一决定，这是因为域的结构比其他代数系更为严紧所致。

二、有限域的乘群

有限域中有两个可换群，一个是域的加群，一个是非零元乘群，后者是结构最简单的群，因为我们有

定理4 有限域F的乘群$\langle F^*,\cdot\rangle$是循环群。

证明：设$|F|=p^t$，a是有限群$\langle F^*,\cdot\rangle$中最大阶元，其阶为n。我们先证明F^*中所有元素的阶都是n的因子，然后证明$\langle a\rangle=\langle F^*,\cdot\rangle$。

任取$b\in F^*$，其阶设为m，假如$m\nmid n$，分两种情况：

(1) m与n互素。这时，$(ab)^{mn}=a^{mn}b^{mn}=1$。另一方面，如果$(ab)^k=1$，则$1=(ab)^{km}=a^{km}b^{km}=a^{km}$。所以$n|km$。由于$m$、$n$互素，故$n|k$。同理$m|k$，即$mn|k$。因而$ab$的阶是$mn>n$，推出矛盾。

(2) m与n不互素。设n，m表为

$$n=p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s},$$
$$m=p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s},$$

其中n_i，m_i为非负整数，p_i为素数。

取$r_i=\mathrm{Max}\{n_i, m_i\}$，$i=1, 2,\cdots,s$。显然$l=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$是$n$，$m$的最小公倍数。由于假定$m\nmid n$，故$l>n$。$p_i^{r_i}$是$n$或$m$的因子，由§3·5定理4，如果$p_i^{r_i}|n$，则$a^{\frac{n}{p_i^{r_i}}}$的阶为$p_i^{r_i}$。如果$p_i^{r_i}|m$，则$b^{\frac{m}{p_i^{r_i}}}$的阶为$p_i^{r_i}$。$p_1^{r_1}, p_2^{r_2}, \cdots, p_s^{r_s}$两两互素，由(1)所证，$F^*$中有阶为$l=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}>n$的元素，与$a$为最大阶元矛盾。

所以，F^*的元素的阶都是n的因子，即F^*的任意元素a适合$a^n=1$，也就是说，a是多项式x^n-1的根。但x^n-1最多有n个根，故$|F^*|=p^t-1\leqslant n$。a在F^*中的阶为n，故$n|p^t-1$，即$n\leqslant p^t-1$，总之，$n=p^t-1=|F^*|$，a所生成的循环群$\langle a\rangle=\langle F^*,\cdot\rangle$。

证毕

定义1 有限域F的非零元乘群$\langle F^*,\cdot\rangle$的生成元，称为

域 F 的本原元。

例 3　写出含 4 个元素的域 F 的运算表。

解：设 α 是 F 的本原元，则 $F=\{0,\ 1,\ \alpha,\alpha^2\}$. 其乘法表如下：$(\alpha^3=1)$

$\cdot$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

F 有一个子域 P 同构于 $\mathbf{Z}_2$，则 F 是多项式 $x^4-x=x(x-1)(x^2+x+1)$ 在 P 上的分裂域。因为 $\alpha\neq1,\ 0$，故 $\alpha^2+\alpha+1=0$，$\alpha+1=-\alpha^2=\alpha^2$（由于 F 的特征为2，F 中任意元素与其负元相等：$0=2a=a+a$，或 $a=-a$），$\alpha^2+1=-\alpha=\alpha$，$\alpha^2+\alpha=-1=1$，所以，加法表为：

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

在本例中，α^2 也是 F 的本原元，所以有限域的本原元是不唯一的。

有限域除了元素个数为 p^n，非零元乘群为循环群等特性外，还有一个重要性质：

三、完全性

定理 5　有限域 F 是完全域。

证明：设 F 的特征为 p，$|F|=p^n$，$F=\{a_1,a_2,\cdots,a_{p^n}\}$. 显然，$a_1^p,\ a_2^p,\cdots,a_{p^n}^p\in F$，且

$$a_i^p-a_j^p=(a_i-a_j)^p\neq0\ \ (i\neq j).$$

因而 $a_1^p,\ a_2^p,\cdots,a_{p^n}^p$ 两两不同，因而正好包含 F 的全部元素，所以 F 中的每个元素都是其中某一元素的 p 次方幂。由上节

定理 3 得证。

证毕

定理 6 有限域 F 的有限代数扩域 E 是单扩域。

证明：显然 E 也是有限域，由定理 5，$\langle E^*, \cdot\rangle$ 是循环群，设 a 是其本原元，所以，$F(a)=E$。

证毕

综合上节定理 4 和本节定理 6，可得

推论 1 任意域的有限可分扩域是单扩域。

四、有限域的子域

有限域所含元素的个数不仅唯一地决定域本身的性质，也唯一地决定其所有子域。

定理 7 设 E 是域，$|E|=p^n$，则 E 的任何子域 F 所含元素的个数为 p^m，其中 $m|n$。反之，对于 n 的任何正因子 m，存在唯一的子域 F，$|F|=p^m$。

证明：设 F 是 E 的子域，由于 E 的特征是 p，所以 F 的特征也是 p。由定理 1，$|F|=p^m$。E 是 F 的扩域。设 P 是 E（也是 F）的素域，则 $[E:P]=[E:F][F:P]$，而 $[E:P]=n$，$[F:P]=m$，所以 $m|n$。

反之，设 $m|n$，则

$$p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\cdots+p^m+1),$$

$p^m-1|p^n-1$.因而 $x^{p^m-1}-1|x^{p^n-1}-1$，或 $x^{p^m}-x|x^{p^n}-x$，$x^{p^n}-x$ 在 E 上可分解为一次因子的乘积，因而 $x^{p^m}-x$ 也可以在 E 上分解为一次因子的乘积，于是 E 中包含 $x^{p^m}-x$ 的全部 p^m 个根，这 p^m 个根刚好形成一个子域（见定理 2 的证明），设为 F，它是 $x^{p^m}-x$ 的分裂域。

假定 F_1 也是 E 的子域，$|F_1| = p^m$，则 F_1 也是多项式 $x^{p^m} - x$ 的分裂域，由于在 E 中同一多项式的分裂域是唯一的，故 $F_1 = F$，即这样的子域是唯一的。

证毕

这样，一个含 p^n 个元素的域，其子域的个正好等于 n 的正因子数。如 $2^4 = 16$ 元域有三个子域，因为 4 有 3 个因子：1，2，4。所以三个子域各含 2、4、16 个元素。

习 题 5·7

1. 举出一个含 125 个元素的域。

2. 如果可换环的素理想 P 只有有限个（$\geqslant 2$）陪集时，P 对应的商环是有限域。

3. 试问 32 个元素的域中有多少本原元？

4. 设 p、q 为素数，求证，含 p^q 个元素的域中除素域外，没有真子域。

5. 设 F 是含 32 个元素的域，$\alpha \in F$，$F = \mathbf{Z}_2(\alpha)$，其中 $\alpha^5 + \alpha^2 + 1 = 0$，试求 α^{-1}。

6. 设 F 是含 27 个元素的域，$\alpha \in F$，$F = \mathbf{Z}_3(\alpha)$，其中 $\alpha^3 + \alpha^2 + 2 = 0$，试求 $(\alpha - 1)(\alpha^2 - 2\alpha)$。

*§5·8 伽罗华理论简介

伽罗华（Galois）注 理论是抽象代数中最负盛名的部分之一，它把域与子域的关系，转化为群与子群的关系。伽罗

注 E. Galois(1811—1832)，法国青年数学家。

华理论成功的应用，使判断代数方程能否用根式求解的问题，得到完满的解决。

这一部分涉及面较广，我们只简述其主要结果，有些定理将略去证明。

一、伽罗华群

设E是域．E的全体自同构关于变换的乘法作成群，是E的一一变换群$G(E)$的子群（见§3·6），这因为自同构的积和逆仍是自同构．E的自同构群记为$A(E)$．

设σ是E的一个自同构．$\sigma(1)=1$，$\sigma(0)=0$，所以1和0是任何自同构的不动元，此外，$n\cdot 1(n\in \mathbf{Z})$显然也是不动元，从而$E$的素域$P$的元素都在$\sigma$下不发生变动．用$I(\sigma)$表示$E$中在$\sigma$下的不动元集合，则$P\subseteq I(\sigma)$．

引理1 $I(\sigma)$是E的子域．

证明：$1\in I(\sigma)$，故$I(\sigma)$含有非零元．设a，$b\in I(\sigma)$，则

$$\sigma(a-b)=\sigma(a)-\sigma(b)=a-b,$$

故$a-b\in I(\sigma)$．

当$b\neq 0$时，

$$\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1}=ab^{-1},$$

故$ab^{-1}\in I(\sigma)$．

由§5·1定理4，$I(\sigma)$是E的子域．

证毕

设$H\subseteq A(E)$．用$I(H)$表示E中对于H的每个元素都不动的元素组成的集合，即

$$I(H)=\{a\in E\mid \sigma(a)=a,\ \sigma\in H\}=\bigcap_{\sigma\in H} I(\sigma).$$

$I(H)$是E的子域的交，自然也是E的子域。

例1　设$E=\mathbf{Q}(\sqrt{2},i)$，$H=\{\varepsilon,\varphi\}$，其中$\varepsilon$是$E$的恒等变换，$\varphi$是这样的自同构：$\varphi(\sqrt{2})=-\sqrt{2}$，$\varphi(i)=-i$。试求$I(H)$和$[E:I(H)]$。

解：取E在$\mathbf{Q}$上的基1，$\sqrt{2}$，i，$\sqrt{2}i$（见§5·4例6）。E的元素形如$\alpha=a_1+a_2\sqrt{2}+a_3i+a_4\sqrt{2}i\ (a_i\in\mathbf{Q})$，$\varphi(\alpha)=a_1-a_2\sqrt{2}-a_3i+a_4\sqrt{2}i$。因而，$\alpha\in I(H)$当且仅当$\alpha$形如$\alpha=a_1+a_4\sqrt{2}i$。即$I(H)=\{\alpha|\alpha=a+b\sqrt{2}i,\ a,\ b\in\mathbf{Q}\}$，它是$\mathbf{Q}$的二次扩域，即$[I(H):\mathbf{Q}]=2$。而$4=[E:I(H)][I(H):\mathbf{Q}]$，所以$[E:I(H)]=2$。

上面说明了域的任意自同构集合将确定一个不动元子域；反之，如果已知域E的一个子域F，则一定存在E的自同构，使F的元素都是它的不动元。事实上，至少恒等变换ε就是这样的一个自同构。设使F的元素不动的自同构组成的集合记为$A(E|F)$。

引理2　$A(E|F)$是$A(E)$的子群。

证明：$\varepsilon\in A(E|F)$，故$A(E|F)\neq\phi$。设$\sigma,\tau\in A(E|F)$，则对于$a\in F$，$\sigma\tau(a)=\sigma(\tau(a))=\sigma(a)=a$，即$\sigma\tau\in A(E|F)$。又由于$\sigma(a)=a$，所以$\sigma^{-1}(a)=a$，即$\sigma^{-1}\in A(E|F)$。因而$A(E|F)$是$A(E)$的子群。

证毕

定义1　$A(E|F)$称为域E在子域F上的伽罗华群。

例2　设$E=\mathbf{Q}(\sqrt[3]{2})$，求$A(E|\mathbf{Q})$。

解：显然$\mathbf{Q}$是E的素域，故对于任意的$\sigma\in A(E)$，有$\mathbf{Q}\subseteq I(\sigma)$。$E$的元素形如$a+b\sqrt[3]{2}+c\sqrt[3]{4}\ (a,b,c\in\mathbf{Q})$。假定$t=\sigma(\sqrt[3]{2})$，则$t^3=2$。而$\sqrt[3]{2}$是唯一满足$x^3=2$的实数，所以

$t=\sqrt[3]{2}$. 因而$\sigma(a+b\sqrt[3]{2}+c\sqrt[3]{4})=\sigma(a)+\sigma(b)t+\sigma(c)t^2$ $=a+b\sqrt[3]{2}+c\sqrt[3]{4}$，即$\sigma=\varepsilon_E$。所以$A(E|Q)$只有一个元素$\varepsilon_E$。

例 3 设$E=Q(\sqrt{2}, i)$，$F=Q(\sqrt{2}i)$，求$A(E|F)$。

解：由$[E:Q]=4$，$[F:Q]=2$，$[E:F]=\frac{[E:Q]}{[F:Q]}=2$。$i\bar{\in}F$。故1，$i$构成$E$在$F$上的一组基。$E$的元素形如$\alpha=a+bi(a, b\in F)$。设$\sigma\in A(E|F)$，则$\sigma(\alpha)=\sigma(a)+\sigma(b)\cdot\sigma(i)=a+b\sigma(i)$。由于$\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1$，故$\sigma(i)=i$或$-i$。设$\sigma_1(i)=i$，则$\sigma_1=\varepsilon_E$。设$\sigma_2(i)=-i$，则$\sigma_2(a+bi)=a-bi$。因而$A(E|F)$是二阶群，即二阶循环群。

二、伽罗华对应

如上所述，对一个固定的域而言，一方面，它的任一子域F将决定$A(E)$中的一个子群（伽罗华群）$A(E|F)$，另一方面，由$A(E)$的任一子群H，也决定E的一个不动元子域$I(H)$。此外，显然有

引理 3 如果F, K是域E的子域，$F\subseteq K$，则对应的伽罗华群有反向包含关系，即$A(E|K)\subseteq A(E|F)$。如果H，J是$A(E)$的子群，$H\subseteq J$，则对应的不动元子域有反向包含关系，即$I(J)\subseteq I(H)$。

证明留给读者。

但是，上述子域与子群的对应还不能断言是一一对应，例如一个子域F的伽罗华群$A(E|F)$的不变元子域$I(A(E|F))$显然包含F，但不能保证等于F。如果将E的条件加强，就可以保证这一点。

定义 2 设 $f(x)$是域 F 上的可分多项式，E是 $f(x)$在 F 上的分裂域，则E在F上的伽罗华群 $A(E|F)$称为多项式 $f(x)$在 F 上的伽罗华群。

如多项式 $x^4-x-2=(x^2-2)(x^2+1)$在 $\mathbf{Q}$ 上的伽罗华群就是 $\mathbf{Q}(\sqrt{2},i)$在 $\mathbf{Q}$ 上的伽罗华群 $A(\mathbf{Q}(\sqrt{2},i)|\mathbf{Q})$。

当E是F上的可分多项式 $f(x)$的分裂域时，前面讲到的子域与子群的对应，有着极好的性质，这就是著名的伽罗华理论基本定理：

定理 1 设E是域F上可分多项式 $f(x)$ 的分裂域，$G=A(E|F)$,则G的所有子群和E的所有含F的子域之间有一一对应，即$K=I(H)$当且仅当$H=A(E|K)$。而且$|H|=[E:I(H)]$，且$(G:H)=[I(H):F]$。

证明从略。

例 4 设 $f(x)=x^2-x-2$, $f(x)$的分裂域是$E=\mathbf{Q}(\sqrt{2},i)$。由于E的特征为∞，故 $f(x)$是可分的。先来计算 $f(x)$的伽罗华群。

设$\sigma\in A(E|F)$.由于 $\sigma(i)^2=\sigma(i^2)=\sigma(-1)=-1$，因而 $\sigma(i)=i$ 或 $-i$， $\sigma(\sqrt{2})^2=\sigma(\sqrt{2}^2)=\sigma(2)=2$，故 $\sigma(\sqrt{2})=\sqrt{2}$或$-\sqrt{2}$。$E$的每个元素可表为

$$a=a_1+a_2\sqrt{2}+a_3i+a_4\sqrt{2}i \quad (a_k\in\mathbf{Q}).$$

因而只要$\sigma(\sqrt{2})$和$\sigma(i)$确定，$\sigma(a)$就完全确定。所以E的自同构共有四个：σ_1，σ_2，σ_3，σ_4。

$$\sigma_1=\varepsilon_E;$$

$$\sigma_2(\sqrt{2})=\sqrt{2},\ \sigma_2(i)=-i;$$

$$\sigma_3(\sqrt{2})=-\sqrt{2},\ \sigma_3(i)=i;$$

$$\sigma_4(\sqrt{2})=-\sqrt{2},\ \sigma_4(i)=-i.$$

易见$\sigma_2^2=\sigma_3^2=\sigma_4^2=\sigma_1=\varepsilon$，$\sigma_2\sigma_3=\sigma_3\sigma_2=\sigma_4$，$\sigma_3\sigma_4=\sigma_4\sigma_3=\sigma_2$，$\sigma_2\sigma_4=\sigma_4\sigma_2=\sigma_3$。由此不难证明$\boldsymbol{A}(E|\boldsymbol{Q})$同构于克莱茵四元群$\boldsymbol{B}_4$。$\boldsymbol{A}(E|\boldsymbol{Q})$共有五个子群：

$$H_1=\{\sigma_1\},\ H_2=\{\sigma_1,\ \sigma_2\},\ H_3=\{\sigma_1,\sigma_3\},$$
$$H_4=\{\sigma_1,\ \sigma_4\},\ H_5=\{\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4\}.$$

下面找出这五个子群在E中对应的不动元子域。

$$I(H_1)=E;$$
$$I(H_2)=I(\sigma_1)\cap I(\sigma_2)=I(\sigma_2)$$
$$=\{a_1+a_2\sqrt{2}\,|a_1,\ a_2\in\boldsymbol{Q}\},$$
$$I(H_3)=I(\sigma_1)\cap I(\sigma_3)=I(\sigma_3)=\{a_1+a_3i\,|a_1,\ a_3\in\boldsymbol{Q}\},$$
$$I(H_4)=I(\sigma_1)\cap I(\sigma_4)=I(\sigma_4)$$
$$=\{a_1+a_4\sqrt{2}\,i\,|a_1,\ a_4\in\boldsymbol{Q}\},$$
$$I(H_5)=I(\sigma_1)\cap I(\sigma_2)\cap I(\sigma_3)\cap I(\sigma_4)=\boldsymbol{Q}.$$

以上五个子域的伽罗华群是：

$$\boldsymbol{A}(E|I(H_1))=\{\sigma_1\}=H_1;$$
$$\boldsymbol{A}(E|I(H_2))=\{\sigma_1,\ \sigma_2\}=H_2;$$
$$\boldsymbol{A}(E|I(H_3))=\{\sigma_1,\ \sigma_3\}=H_3;$$
$$\boldsymbol{A}(E|I(H_4))=\{\sigma_1,\ \sigma_4\}=H_4;$$
$$\boldsymbol{A}(E|I(H_5))=\{\sigma_1,\ \sigma_2,\ \sigma_3,\ \sigma_4\}=H_5.$$

此外，易见

$$[E:I(H_1)]=1=|H_1|;$$
$$[E:I(H_2)]=2=|H_2|;$$
$$[E:I(H_3)]=2=|H_3|;$$
$$[E:I(H_4)]=2=|H_4|;$$
$$[E:I(H_5)]=4=|H_5|.$$

伽罗华理论基本定理中的子域与子群的一一对应关系，

称为伽罗华对应．借助这一对应，域的问题转化为群的问题．它的一个重要应用是用多项式的伽罗华群的性质来判断对应的代数方程能否用根式求解．为了说明这个问题，必须首先明确什么是根式求解．

三、根式求解

我们知道，若数域 F 上的一个代数方程

$$f(x)=0$$

的所有根能由 F 中的数经有限次加、减、乘、除和开方得到，就称这个方程可用根式求解．如二、三、四次方程都可以用根式求解．

但是，上面关于根式求解的说法不够准确，例如什么是开方，在一般的域 F 上代表什么意思，难以说清．以下引进

定义 3 设有域 F 上的多项式 $f(x)$．如果存在域列：

$$F=F_1\subseteq F_2\subseteq\cdots\subseteq F_{r+1}=E,$$

其中 $F_2=F_1(d_1)$，d_1 是 $x^{n_1}-a_1$ 的根，$a_1\in F$，$F_3=F_2(d_2)$，d_2 是 $x^{n_2}-a_2$ 的根，$a_2\in F_2,\cdots,F_{r+1}=F_r(d_r),d_r$ 是 $x^{n_r}-a_r$ 的根，$a_r\in F_r$，且 E 包括 $f(x)$ 的所有根，即 E 包含 $f(x)$ 的分裂域，这时称方程 $f(x)=0$ 可以在 F 上用根式求解．

那末，什么样的代数方程能用根式求解呢？

四、伽罗华准则

定理 2 特征为 ∞ 的域 F 上的代数方程 $f(x)=0$ 能用根式求解的充要条件是 $f(x)$ 在 F 上的伽罗华群是可解群．（证明从略）

因而方程根式求解问题归为群论中的问题．下面，我们

来分析多项式的伽罗华群。

设有域 F（特征为 ∞）上的多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n$，$E$ 是其分裂域，$E=F(\alpha_1,\cdots,\alpha_n)$，设 $f(x)$ 无重根，$\sigma\in A(E|F)$，则

$$0=\sigma(f(\alpha_i))=\sigma(a_0)+\sigma(a_1)\sigma(\alpha_i)+\cdots+\sigma(a_n)\sigma(\alpha_i)^n$$
$$=a_0+a_1\sigma(\alpha_i)+\cdots+a_n\sigma(\alpha_i)^n.$$

因而 $\sigma(\alpha_i)$ 仍是 $f(x)$ 的根。所以 $\sigma(\alpha_i)\in R=\{\alpha_1,\cdots,\alpha_n\}$。由于 σ 是一一变换，所以不同的 α_i 在 σ 下的象 $\sigma(\alpha_i)$ 也不相同，即 σ 决定一个置换

$$\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix},$$

这里假定 $\sigma(\alpha_1)=\alpha_{i_1}$，$\sigma(\alpha_2)=\alpha_{i_2},\cdots$，$\sigma(\alpha_n)=\alpha_{i_n}$。设 τ 对应的置换是 $\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}$，则

$$\sigma\tau(\alpha_k)=\sigma(\alpha_{j_k})=\alpha_{i_{j_k}}$$

即 $\quad\sigma\tau\to\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}.$

所以，上述由 σ 这样来确定 n 次置换的方法作成 $A(E|F)$ 到 S_n 的一个同态映射，其同态象是 S_n 的一个子群。显然不同的自同构确定的置换也不相同。所以这一同态是同构，$A(E|F)$ 同构于 S_n 的一个子群，即 n 次置换群，也可以直接称这个置换群为 $f(x)$ 的伽罗华群，这就是说，无重根的多项式的伽罗华群是一个 n 次置换群。

因而低于五次的多项式的伽罗华群总是 S_2、S_3 及 S_4 的一个子群，因而是可解群（见 § 3·14），根据伽罗华准则，低于五次的方程可用根式求解。而当 $n\geqslant5$ 时，S_n 的子群中有

可解群也有不可解群，所以，高于四次的方程有的可以用根式求解，有的不能用根式求解。如 x^5+px+p（p 是任意素数）的伽罗华群可以证明是 S_5，S_5 不是可解群，因而 $x^5+px+p=0$ 不能用根式求解。而方程 $x^5-1=0$ 却可以用根式求解。

五、阿贝尔定理

方程

$$x^n+t_1x^{n-1}+\cdots+t_n=0, \tag{1}$$

其中 $t_1,\cdots,t_n$ 是域 F 的无关超越元（即每个 t_i 是扩域 $F(t_1,\cdots,t_{i-1},t_{i+1},\cdots,t_n)$ 的超越元），称为域 F 上的 n 次一般方程。记超越扩域 $F(t_1,\cdots,t_n)=K$，如果方程（1）可以在 K 上用根式求解，则根可以用公式表达，即有求根公式。二、三、四次方程有一般的求根公式，更高次的却没有。

定理 3 （阿贝尔定理）n 次一般方程（1）的伽罗华群是 S_n，因而当 $n>4$ 时不能用根式求解，即没有求根公式（假定 F 的特征为 ∞）。

本 章 提 要

一、域的特征：非零元在加群中的阶。它或为素数或为 ∞。

二、分式域：无零因子的可换环存在分式域，其元素可写成环中两元素的商，分式域可以认为是包含环的最小域，它在不计同构的意义下是唯一的。

三、单代数扩域 $F(\alpha)$：由一切形如 $a_0+a_1\alpha+\cdots+$

$a_{n-1}\alpha^{n-1}$ （$a_i\in F$）的元素组成。 $F(\alpha)\cong F[x]/\langle p(x)\rangle$。其中 $p(x)$是 α 在 F 上的极小多项式。

四、单超越扩域 $F(\alpha)$：由一切形如 $\dfrac{a_0+a_1\alpha+\cdots+a_n\alpha^n}{b_0+b_1\alpha+\cdots+b_m\alpha^m}$ （a_i，$b_j\in F$）的元素组成。$F(\alpha)\cong F(x)$（F 上的有理分式域）。

五、代数扩域：由代数元组成的扩域。

六、有限扩域：作为向量空间维数有限的扩域。有限扩域是代数扩域，反之不然。有限扩域的有限扩域仍是有限扩域，且次数为两次扩域次数之积。

七、分裂域：F 上的多项式 $f(x)$可以分解为一次因子的 F 的最小扩域。分裂域总是存在的，在同构的意义下也是唯一的。

八、可分扩域：扩域的任意元素的极小多项式无重根。任意有限可分扩域是单扩域。

九、有限域：含 p^n（p——素数）个元素的域，其特征为 p，它是素域上多项式 $x^{p^n}-x$ 的分裂域，其非零元乘群是循环群，子域也是含有 p^m（$m\leqslant n$）个元素的域。

复 习 题 五

1．设 α 在域 F 上的极小多项式是 $p(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n$。求 α 在 $F(\alpha)$中的逆元。

2．求证：在特征为 2 的域中，$a=-a$。

*3．设 K 是域 F 的二次扩域，求证：存在 $w\in F$，使 $K=F(v)$，其中 v 是 x^2-w 的根。

*4. 设 F 是 $\mathbf{R}$ 的有限扩域，求证：$F\cong\mathbf{R}$ 或 $F\cong\mathbf{C}$.

5. 设域 F 的特征为 p，$\alpha^{p^n}=\gamma\in F$，但 $\alpha^{p^{n-1}}\in F$，求证：多项式 $x^{p^n}-\gamma$ 在 $F[x]$ 中既约。

*6. 求证：完全域的代数扩域也是完全域。

7. $\mathbf{Q}(\sqrt{2})$，$\mathbf{Q}(\sqrt{3})$，$\mathbf{Q}(i)$ 是否 $\mathbf{Q}$ 的等价扩域？

8. 设域 F 的特征为 p，$E=F(\alpha)$，α 是 $F[x]$ 中多项式 x^p-a 的根，求证：$F(\alpha)$ 是 x^p-a 的分裂域。

9. 设 $p(x)$ 和 $q(x)$ 是域 F 上的首项系数为 1 的既约多项式，求证：F 有有限扩域 $F(\alpha_1, \alpha_2)$，使 α_1, α_2 的极小多项式分别为 $p(x)$ 和 $q(x)$。

10. 求证：x^3-2 在 $\mathbf{Q}(\sqrt{3})$ 上既约。

*11. 设 E 是域 F 的有限代数扩域，$f(x)$ 是 E 上的既约多项式。求证：在 $F[x]$ 中有既约多项式 $q(x)$，使在 $E[x]$ 中 $f(x)\mid q(x)$。

12. 求证：$\mathbf{Q}(\alpha)$ 不是多项式 x^3-a 在 $\mathbf{Q}$ 上的分裂域。其中 α 是 x^3-a 的一个根。

*13. 设 E 是域 F 的扩域，K 是 E 的扩域，K 的元素 α 在 F 上的次数与 E 关于 F 扩域的次数互素，求证：α 在 E 上的次数与 α 在 F 上的次数相等。

第六章　代数和模

代数，是我们这门学科的名称，也是一类代数系的名称。代数这类代数系根据其不同性质又分为许多分支，发展成为若干专门学科，它们在分析、几何以及物理中应用很广。这一章除介绍代数的最初步的知识外，还用很少的篇幅介绍另一类重要的代数系——模。

§6·1　代数的基本概念

一、什么是代数？

我们知道，实向量空间 V 中的全体线性变换又构成一个新的实向量空间 L．L 关于线性变换的乘法封闭，即作成乘群胚，乘法关于线性变换的加法有分配律，且对于任何 $a\in \mathbf{R}$，σ，$\tau\in L$，有 $a(\sigma\tau)=(a\sigma)\tau=\sigma(a\tau)$。

L 是代数的最基本的例子．一般地，有

定义 1　设 F 是域，A 是 F 上的向量空间（见§5·4定义1），同时 A 有乘法运算，乘法关于加法有分配律，且对于 a，$b\in A$，$k\in F$，有

$$k(ab)=(ka)b=a(kb)。\tag{1}$$

这时，称 A 为域 F 上的代数．

代数 A 的乘群胚 $\langle A,\cdot\rangle$ 如果是半群（乘法适合结合律），则称 A 为结合代数，否则称非结合代数。结合代数既是环又

是向量空间。代数的乘法如果是可换的，则称为可换代数，否则称不可换代数。代数关于乘法如果有单位元，则称有单位元代数。代数A如果对于任意的$a\neq 0$和b，方程$ax=b$，$ya=b$都有唯一解，则称A为可除代数。可除的结合代数是体，可换可除的结合代数显然是域。

代数A作为F上向量空间的维数，称为A的次数。

例 1 设$F[x]$是域F上的多项式环。对于$f(x)\in F[x]$，$a\in F\subseteq F[x]$，总有$af(x)\in F[x]$，$F[x]$作成F上的向量空间，且显然乘法有结合律，乘法关于加法有分配律，而且有

$$a(f(x)g(x))=(af(x))g(x)=f(x)(ag(x)).$$

所以$F[x]$是F上的结合代数。$F[x]$的单位元即F的单位元1．$F[x]$是无限次的，因为$\{1, x, x^2, \cdots\}$是线性无关的集合。$F[x]$显然是可换代数，但不是可除代数。

例 2 设E是域F的扩域，E可看作F上的向量空间。此外，(1)式显然成立，且乘法关于加法有分配律，而E^*是可换群，所以E是F上的可换可除的结合代数。

例 3 设$M_n(F)$是域F上的所有n阶方阵组成的集合，$M_n(F)$是环(见§4·1)。规定

$$k(a_{ij})=(ka_{ij})\quad (k\in F,\ (a_{ij})\in M_n(F))$$

则显然$M_n(F)$作成F上的结合代数，其单位元为单位方阵，次数为n^2，$M_n(F)$是不可换的也是不可除的。

例 4 设$\boldsymbol{R}_3$为实三维向量空间，规定$\boldsymbol{R}_3$的乘法为几何中的向量积(或称外积)：

$$(a_1, a_2, a_3)\times(b_1, b_2, b_3)$$
$$=(a_2b_3-a_3b_2,\ a_3b_1-a_1b_3,\ a_1b_2-a_2b_1).$$

易见，乘法对于加法的分配律成立，(1)式也成立。所以$\boldsymbol{R}_3$作

成实数域上的三次代数．它不是结合的，如[(1, 0, 0) $\times$ (0,1,0)] $\times$ (0,1,0) = (−1,0,0) $\neq$ (0, 0, 0) = (1, 0, 0) $\times$ [(0,1,0) $\times$ (0,1,0)]，也不是可换的，如(1,0,0) $\times$ (0,1,0) = (0,0,1) $\neq$ (0,0,−1) = (0,1,0) $\times$ (1,0,0)．乘法没有单位元，因为对于任何$(a_1, a_2, a_3) \in \boldsymbol{R}_3$，有

$$(a_1, a_2, a_3) \times (a_1, a_2, a_3) = (0,0,0).$$

二、由基决定代数

如果A是域F上的n次代数，α_1，α_2，…，α_n是A的一组基，则A中的每个元素可以唯一地表为$a = \sum_{i=1}^{n} k_i \alpha_i$，$k_i \in F$．基元素$\alpha_i$，$\alpha_j$的乘积$\alpha_i \alpha_j \in A$，因而也可以用基来表示：

$$\alpha_i \alpha_j = \sum_{s=1}^{n} t_{ij}^s \alpha_s, \quad i, j = 1, 2, \cdots, n.$$

t_{ij}^s共有n^3个，它们由A中的乘法唯一决定．称为A的结构常数．如果知道了这n^3个结构常数，A中任意两个元素的乘积也就唯一决定了．事实上，设$a = \sum_{i=1}^{n} k_i \alpha_i$，$b = \sum_{j=1}^{n} l_j \alpha_j$，那末

$$\begin{aligned} ab &= \left(\sum_{i=1}^{n} k_i \alpha_i\right)\left(\sum_{j=1}^{n} l_j \alpha_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} (k_i \alpha_i)(l_j \alpha_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} k_i l_j \left(\sum_{s=1}^{n} t_{ij}^s \alpha_s\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{s=1}^{n} (k_i l_j t_{ij}^s) \alpha_s \\ &= \sum_{s=1}^{n} \left(\sum_{i=1}^{n} \sum_{j=1}^{n} k_i l_j t_{ij}^s\right) \alpha_s. \end{aligned}$$

由此可以看出，基元素之间乘积的性质，将决定整个代

数的性质。具体说来，就是以下两个定理：

定理1 设A为域F上的代数。A为结合代数的充要条件是对于任意的基元素α_i，α_j，α_s，有

$$(\alpha_i\alpha_j)\alpha_s = \alpha_i(\alpha_j\alpha_s)。\tag{2}$$

证明：设A为结合代数，由于基元素也应适合结合律，故(2)式成立。

反之，如果（2）式成立，任取$\sum_{i=1}^{n} a_i\alpha_i$，$\sum_{i=1}^{n} b_i\alpha_i$，$\sum_{i=1}^{n} c_i\alpha_i \in A$，则

$$\left(\sum_{i=1}^{n} a_i\alpha_i \cdot \sum_{i=1}^{n} b_i\alpha_i\right)\cdot\left(\sum_{i=1}^{n} c_i\alpha_i\right)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} a_ib_j(\alpha_i\alpha_j)\cdot\sum_{s=1}^{n} c_s\alpha_s$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{s=1}^{n}(a_ib_j)c_s[(\alpha_i\alpha_j)\alpha_s]$$

而

$$\left(\sum_{i=1}^{n} a_i\alpha_i\right)\cdot\left(\sum b_i\alpha_i \cdot \sum_{i=1}^{n} c_i\alpha_i\right)$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{s=1}^{n} a_i(b_jc_s)[\alpha_i(\alpha_j\alpha_s)]。$$

由于（2）式，故以上两式相等，A为结合代数。

证毕

定理2 设A为域F上的代数。A为可换代数的充要条件是对于任意的基元素α_i，α_j，有

$$\alpha_i\alpha_j = \alpha_j\alpha_i。\tag{3}$$

证明类似定理1，留作练习。

三、群代数

如果已知域 F 和有限群胚 $G=\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. 以下作出 F 上的 n 次代数，使 A 的一组基是 G。

取 $A=\{a_1\alpha_1+\cdots+a_n\alpha_n \mid a_i\in F\}$，并规定：

$$a_1\alpha_1+\cdots+a_n\alpha_n=0 \Longleftrightarrow a_1=\cdots=a_n=0;$$

$$k(a_1\alpha_1+\cdots+a_n\alpha_n)=ka_1\alpha_1+\cdots+ka_n\alpha_n, \quad (k\in F);$$

$$\begin{aligned}&(a_1\alpha_1+\cdots+a_n\alpha_n)+(b_1\alpha_1+\cdots+b_n\alpha_n)\\ =&(a_1+b_1)\alpha_1+\cdots+(a_n+b_n)\alpha_n;\end{aligned}$$

$$\begin{aligned}&(a_1\alpha_1+\cdots+a_n\alpha_n)(b_1\alpha_1+\cdots+b_n\alpha_n)\\ =&a_1b_1\alpha_1^2+\cdots+a_1b_n(\alpha_1\alpha_n)+\cdots\\ &+a_nb_1(\alpha_n\alpha_1)+\cdots+a_nb_n\alpha_n^2.\end{aligned}$$

（其中 $\alpha_i\alpha_j$ 等于群胚 G 中的结果）

约定 α_i 看作 $0\alpha_1+\cdots+1\alpha_i+\cdots+0\alpha_n$，则易见 A 中元素 $a_1\alpha_1+\cdots+a_n\alpha_n$ 与 A 中的上述运算也是一致的。这时，G 是 A 的一组基。A 称为群胚 G 在域 F 上的群胚代数，记为 $F(G)$。当 G 为半群时，由定理 1，$F(G)$ 是结合代数；当 G 为群时，$F(G)$ 称为群代数。群代数是有单位元的结合代数。

例 5 三阶循环群 $\langle a\rangle=\{a^0=e, a, a^2\}$ 在域 $\mathbf{Z}_2$ 上的群代数包含以下形式的元素：

$$\alpha=k_0e+k_1a+k_2a^2 \quad (k_0, k_1, k_2\in\mathbf{Z}_2).$$

$\mathbf{Z}_2$ 只有两个元素[0]、[1]，简记为 0、1，所以 A 有 $2^3=8$ 个元素，其运算举例如下：

$$\begin{aligned}&(e+a+a^2)+(e+a^2)\\ =&(1+1)e+(1+0)a+(1+1)a^2=a^2,\end{aligned}$$

$$(e+a+a^2)(e+a^2)=e+a^2+a+e+a^2+a=0.$$

由此可见，$e+a+a^2$ 无逆元，所以 A 不是可除代数。

习 题 6·1

1. $\mathbf{C}$ 是 $\mathbf{C}$ 上的几次代数？
2. 写出二阶循环群在 $\mathbf{Z}_2$ 上的群代数运算表。
3. 证明本节定理 2。
4. 在域 F 上的代数 A 中，求证：

$$a(kb+lc)=k(ab)+l(ac);$$

$$(kb+lc)a=k(ba)+l(ca).$$

其中 a，b，$c\in A$、k，$l\in F$。

5. 设群胚 $G=\{a,b,c\}$ 的乘法表为：

$\cdot$	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

求证：G 在任意域上的群胚代数是结合代数。

§6·2 代数的基本性质

这一节介绍子代数、理想、商代数、代数的同态与同构，最后，略述代数的矩阵表示。

一、子代数与理想

域 F 上的代数 A 的非空子集 B 如果关于 A 的运算也是 F 上的代数，则称为 A 的子代数，

B是A的子代数，包含以下含义：

(1) 如果b_1，$b_2 \in B$，则$b_1 - b_2$，$b_1 b_2 \in B$；

(2) 如果$b \in B$，$k \in F$，则$kb \in B$。

当A为结合代数时，B是A的子代数等价于说B是向量空间A的子空间，B是环A的子环。

任何代数总有子代数。如$\{0\}$和A都是A的子代数，称为A的平凡子代数，其他子代数称为真子代数。

设S是代数A的子集，包含S的所有子代数的交集显然也是子代数，称之为S生成的子代数。

代数A作为向量空间的子空间不一定是A的子代数。如$B = \{bi \mid b \in \mathbf{R}\}$是$\mathbf{R}$上的二次代数$\mathbf{C}$的子空间，但不是子代数，$ii = -1 \overline{\in} B$。

代数A的子代数I，如果适合条件：对于$a \in A$，$b \in I$，总有$ab \in I$，$ba \in I$，则称I为A的理想。

例 1 任何代数的平凡子代数都是理想，称为平凡理想。

例 2 域F上的有单位元e的代数A中，集合$Fe = \{ke \mid k \in F\}$是A的子代数。

事实上，$ke - le = (k-l)e \in Fe$，$ke \cdot le = kle^2 = kle \in Fe$，$l(ke) = lke \in Fe$，故$Fe$是子代数。

例 3 域F上的结合代数A中与所有元素可换的元素组成的集合设为C，即

$$C = \{a \in A \mid ax = xa, \ x \in A\},$$

称C为A的中心。易证C是可换子代数。例 2 中Fe包含在C中，是C的子代数。

例 4 $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \ a, \ b \in \mathbf{R} \right\}$是$M_2(\mathbf{R})$的子代数。

事实上，我们有

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = \begin{pmatrix} a-a_1 & b-b_1 \\ -(b-b_1) & a-a_1 \end{pmatrix} \in A,$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} = \begin{pmatrix} aa_1-bb_1 & ab_1+ba_1 \\ -(ab_1+ba_1) & aa_1-bb_1 \end{pmatrix} \in A,$$

$$k\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} ka & kb \\ -kb & ka \end{pmatrix} \in A, \quad (k \in \mathbf{R}).$$

所以，A是 $M_2(\mathbf{R})$的子代数。

显然，结合代数或可换代数的子代数，也是结合代数或可换代数。

二、同态

设A和B是域F上的代数，φ 是A到B的映射。如果对于任意 $a, b \in A, k \in F$，有

$$\varphi(ka) = k\varphi(a), \quad \varphi(a+b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b),$$

则称 φ 是代数A到代数B的同态。如果 φ 又是一一映射，则称 φ 为同构，这时称A与B同构，记为 $A \cong B$。与环、群类似，也可以定义满同态、单同态、自同构、自同态等。

例 5 $\mathbf{R}$上的代数$\mathbf{C}$与例 4 的子代数A同构。

证明：作$\mathbf{C}$到A的映射 φ 为 $\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$，显然 $\varphi(k(a+bi)) = \varphi(ka+kbi) = \begin{pmatrix} ka & kb \\ -kb & ka \end{pmatrix} = k\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = k\varphi(a+bi)$。

同样可证

$$\varphi((a+bi)+(a_1+b_1i))=\varphi(a+bi)+\varphi(a_1+b_1i),$$

$$\varphi((a+bi)(a_1+b_1i))=\varphi(a+bi)\varphi(a_1+b_1i).$$

所以 φ 是 $\mathbf{C}$ 到 A 的同态，且显然是一一映射，因而是同构。

三、商代数

设 I 是 F 上代数 A 的理想，则在加群 $\langle A,+\rangle$ 中，I 是子群，陪集 $a+I=\{a+b\mid b\in I\}(a\in A)$ 的集合是商加群 A/I。在 A/I 中

$$(a+I)+(b+I)=(a+b)+I. \tag{1}$$

如果此外补充规定

$$(a+I)\cdot(b+I)=a\cdot b+I, \tag{2}$$

$$k(a+I)=ka+I,\ (k\in F). \tag{3}$$

由于 A/I 是商加群，故(1)是代数运算.(2)和(3)也是 A/I 的代数运算。事实上，若 $a+I=a_1+I$，$b+I=b_1+I$，则 $a_1b_1-ab=a_1b_1-a_1b+a_1b-ab=a_1(b_1-b)+(a_1-a)b\in I$，即 $a_1b_1+I=ab+I$；$ka_1-ka=k(a_1-a)\in I$，因而 $ka_1+I=ka+I$。

定理 1 A/I 按照法则(1)～(3)作成 F 上的代数。

证明类似商环、商群定理，请读者自证。

上述 A/I 称为代数 A 关于理想 I 的商代数。

类似于环的相应结果，可以证明

定理 2 设 A 和 B 是 F 上的代数，φ 是 A 到 B 的同态，$K_\varphi=\varphi^{-1}[0]$(称为同态核)，则 K_φ 是 A 的理想；$\varphi[A]$ 是 B 的子代数且同构于商代数 A/K_φ；$A\cong B$ 当且仅当 $K_\varphi=\{0\}$ 且 φ 为满射。

定理 3 代数 A 与其任意商代数 A/I 同态。

证明当作练习。

设 A 是 F 上的 n 次代数，I 是理想在 F 上的次数设为 m，那末 A/I 是 F 上的几次代数呢？

定理 4 A/I 是 F 上的 $n-m$ 次代数。

证明：设 A/I 是 t 次的，$a_1+I, a_2+I, \cdots, a_t+I$ 是 A/I 的一组基，$b_1, b_2, \cdots, b_m$ 是 I 的一组基，则 $a_1, a_2, \cdots, a_t, b_1, b_2, \cdots, b_m$ 是 A 中线性无关的元素。事实上，如果有等式

$$k_1a_1+\cdots+k_ta_t+l_1b_1+\cdots+l_mb_m=0(k_i, l_i\in F), \qquad (4)$$

则
$$k_1a_1+\cdots+k_ta_t=-(l_1b_1+\cdots+l_mb_m)\in I,$$

即
$$k_1(a_1+I)+\cdots+k_t(a_t+I)=0+I(A/I\text{ 的零元})。$$

由于 $a_1+I, \cdots, a_t+I$ 是 A/I 的基，所以线性无关，故 $k_1=\cdots=k_t=0$，代入(4)式，得 $l_1b_1+\cdots+l_mb_m=0$，即 $l_1=\cdots=l_m=0$。

下面证明 A 的元素可由 $a_1, \cdots, a_t, b_1, \cdots, b_m$ 线性表示。任取 $a\in A$，则 $a+I\in A/I$，故有等式

$$a+I=k_1(a_1+I)+\cdots+k_t(a_t+I), \quad k_i\in F,$$

因而 $a-(k_1a_1+\cdots+k_ta_t)\in I$。于是 $a-(k_1a_1+\cdots+k_ta_t)=l_1b_1+\cdots+l_mb_m(l_i\in F)$，$a=k_1a_1+\cdots+k_ta_t+l_1b_1+\cdots+l_mb_m$。

总之，$a_1, \cdots, a_t$，b_1，$\cdots$，b_m 是 A 的基，A 的次数是 $t+m$。因为 A 是 n 次的，故 $n=t+m$，$t=n-m$。

证毕

四、结合代数的正则矩阵表示

我们知道，域 F 上的 n 阶方阵代数 $M_n(F)$ 是 F 上的结

合代数．下面，我们证明方阵代数实际上也概括了极为广泛的一类代数．这就是

定理 5 设 A 是域 F 上的有单位元的 n 次结合代数，则 A 同构于 $M_n(F)$ 的一个子代数．

证明： 设 A 的基为 $\alpha_1=e$，$\alpha_2,\cdots$，α_n．

任取 $a\in A$．乘积

$$\alpha_1 a,\ \alpha_2 a,\cdots,\ \alpha_n a$$

用 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 表示，可得等式

$$\left\{\begin{array}{l}\alpha_1 a=a_{11}\alpha_1+a_{12}\alpha_2+\cdots+a_{1n}\alpha_n,\\ \alpha_2 a=a_{21}\alpha_1+a_{22}\alpha_2+\cdots+a_{2n}\alpha_n,\\ \cdots\cdots\cdots\cdots\\ \alpha_n a=a_{n1}\alpha_1+a_{n2}\alpha_2+\cdots+a_{nn}\alpha_n.\end{array}\right. \tag{5}$$

$$(a_{ij}\in F)$$

设

$$M_a=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ & & \cdots\cdots\cdots\cdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{pmatrix}\in M_n(F).$$

规定 A 到 $M_n(F)$ 的映射 φ 为 $\varphi(a)=M_a$．

φ 为单射．事实上，如果 $\varphi(a)=\varphi(b)$，则 $M_a=M_b$，M_a-M_b 为零方阵，设 $M_b=(b_{ij})$，那末

$$\begin{aligned}a-b&=e(a-b)=\alpha_1(a-b)\\ &=(a_{11}-b_{11})\alpha_1+(a_{12}-b_{12})\alpha_2+\cdots+(a_{1n}-b_{1n})\alpha_n.\end{aligned}$$

$a_{11}-b_{11}$，$a_{12}-b_{12}$，$\cdots,a_{1n}-b_{1n}$ 是零方阵的一行，所以都是零，因而 $a-b=0$，$a=b$．

φ 是同态．事实上，如果

$$\begin{cases} \alpha_1 b = b_{11}\alpha_1 + b_{12}\alpha_2 + \cdots + b_{1n}\alpha_n, \\ \alpha_2 b = b_{21}\alpha_1 + b_{22}\alpha_2 + \cdots + b_{2n}\alpha_n, \\ \cdots\cdots\cdots\cdots \\ \alpha_n b = b_{n1}\alpha_1 + b_{n2}\alpha_2 + \cdots + b_{nn}\alpha_n, \end{cases}$$

$$(b_{ij} \in F)$$

则

$$\varphi(a+b) = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots & a_{nn}+b_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots\cdots\cdots\cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \cdots\cdots\cdots\cdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix}$$

$$= \varphi(a) + \varphi(b).$$

由于 $\alpha_i(ab) = (\alpha_i a)b = (a_{i1}\alpha_1 + a_{i2}\alpha_2 + \cdots + a_{in}\alpha_n)b$

$$= a_{i1}(\alpha_1 b) + \cdots + a_{in}(\alpha_n b)$$

$$= a_{i1}(b_{11}\alpha_1 + \cdots + b_{1n}\alpha_n) + \cdots$$

$$+ a_{in}(b_{n1}\alpha_1 + \cdots + b_{nn}\alpha_n)$$

$$= (a_{i1}b_{11} + \cdots + a_{in}b_{n1})\alpha_1 + \cdots$$

$$+ (a_{i1}b_{1n} + \cdots + a_{in}b_{nn})\alpha_n.$$

$$(i = 1, 2, \cdots, n)$$

所以

$$\varphi(ab) = M_{ab} = \begin{pmatrix} a_{11}b_{11} + \cdots + a_{1n}b_{n1} & \cdots & a_{11}b_{1n} + \cdots + a_{1n}b_{nn} \\ \cdots\cdots\cdots\cdots \\ a_{n1}b_{11} + \cdots + a_{nn}b_{n1} & \cdots & a_{n1}b_{1n} + \cdots + a_{nn}b_{nn} \end{pmatrix}$$

$$=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & & \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

$$=M_a\cdot M_b=\varphi(a)\varphi(b).$$

任取 $k\in F$，则

$$\alpha_i(ka)=k(\alpha_i a)$$

$$=ka_{i1}\alpha_1+\cdots+ka_{in}\alpha_n.(i=1,2,\cdots,n)$$

$$\varphi(ka)=\begin{pmatrix} ka_{11} & \cdots & ka_{1n} \\ \cdots & \cdots & \cdots \\ ka_{n1} & \cdots & ka_{nn} \end{pmatrix}=kM_a=k\varphi(a).$$

总之，φ 是 A 到 $\varphi[A]\subseteq M_n(F)$的同构映射.

证毕

由定理 2，$\varphi[A]$是 $M_n(F)$的子代数，$\varphi[A]$和 A 在 F 上的次数相同，为 n，而 $M_n(F)$是 F 上的 n^2 次代数，所以一般说来 $\varphi[A]\neq M_n(F)$.

上述 A 到 $\varphi[A]$的同构映射 φ 称为 A 在 $M_n(F)$ 中的正则表示，$\varphi[A]$称为表示的象集.

例 6　写出 $\boldsymbol{C}$ 在 $M_2(\boldsymbol{R})$中的正则表示.

解：取 1，i 为 $\boldsymbol{C}$ 的一组基. 任取 $a+bi\in\boldsymbol{C}$，则 $1(a+bi)=a+bi$，$i(a+bi)=-b+ai$. 所以 $\varphi(a+bi)=\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ 是 $\boldsymbol{C}$ 在 $M_2(\boldsymbol{R})$中的正则表示. 表示的象集 $\varphi[A]=\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\middle| a,b\in\boldsymbol{R}\right\}$，是例 4 所说的子代数，这与例 5 结果一致.

例 7　设 G 是 n 阶循环群$\langle a\rangle$. 写出群代数 $F(G)$ 在 $M_n(F)$中的正则表示.

证明：任取 $\alpha = a_1e + a_2a + \cdots + a_na^{n-1} \in F(G)$ 则

$$\begin{cases} e\alpha = a_1e + a_2a + \cdots + a_na^{n-1}, \\ a\alpha = a_1a + a_2a^2 + \cdots + a_na^n, \\ \cdots\cdots\cdots\cdots \\ a^{n-1}\alpha = a_1a^{n-1} + a_2a^n + \cdots + a_na^{2n-2}, \end{cases}$$

所以

$$\varphi(\alpha) = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \cdots\cdots\cdots\cdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix}$$

上面的方阵每行为 $a_1, a_2, a_3, \cdots, a_n$ 的一个轮转，平行于主对角线的每条斜线由同一元素组成，共 $2n-1$ 条斜线，元素依次为：$a_2, a_3, \cdots, a_n$，a_1（对角线），$a_2, \cdots, a_n$。反之，任取 F 中 n 个元素 a_1，$a_2, \cdots$，a_n，按上述规律组成的 n 阶方阵一定是 $F(G)$ 中元素 $a_1e + a_2a + \cdots + a_na^{n-1}$ 的象。所以，象集 $\varphi[F(G)]$ 由 F 上一切具有上述规律的 n 阶方阵组成。这种方阵常称循环方阵。

代数的正则矩阵表示，可以使代数的讨论转化为矩阵的讨论。

习 题 6·2

1．设 H 是有限群 G 的子群，H 在任意域 F 上的群代数是否 G 在 F 上群代数的子代数？

2．找出 $\mathbf{C}$ 作为 $\mathbf{R}$ 上代数的所有子代数。

3．求证：域 F 上的多项式代数 $F[x]$ 中常数项为 0 的

多项式集 $F_0[x]$是理想。

4. 设 x 是代数 A 的固定元素，求证：包含 x 的最小理想是 $I_x=\left\{\sum_{i=1}^{n} a_i x b_i \mid a_i, b_i \in A,\ n\in \boldsymbol{P}\right\}$。

5. 如果 A 是结合代数，I 是它的理想，求证：商代数也是结合代数。

6. 证明本节定理 2 和定理 3。

7. 写出克莱因四元群 B_4 在 $\boldsymbol{R}$ 上的群代数在 $M_4(\boldsymbol{R})$ 中的正则表示（见 § 3·1 例 4）。

§ 6·3　四元数代数

本节先介绍四元数代数 $\boldsymbol{H}$，然后证明它是 $\boldsymbol{R}$ 上除 $\boldsymbol{R}$ 和 $\boldsymbol{C}$ 外唯一的有限次可除结合代数。

一、什么是四元数代数？

设 $\boldsymbol{H}$ 是实数域 $\boldsymbol{R}$ 上以 1，i，j，k 为基的四维向量空间，其中 $1\in \boldsymbol{R}$，i，j，$k\notin \boldsymbol{R}$，即 $\boldsymbol{H}=\{a+bi+cj+dk \mid a, b, c, d\in \boldsymbol{R}\}$，基元素的乘法表为：

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$\boldsymbol{H}$ 作成 $\boldsymbol{R}$ 上的 4 次代数。

$\boldsymbol{H}$ 不可换，如

$$ij=k\neq -k=ji.$$

为了证明 $\boldsymbol{H}$ 是结合代数，由定理 1，只须验证基元素 1，i，j，k 关于乘法适合结合律，而 i，j，k 在乘法表中所处的地位显然完全对称，所以只须验

证以下几种情形：

$(ii)i=i(ii)$，$(ii)j=i(ij)$，

$(ij)i=i(ji)$，$(ji)i=j(ii)$，

$(ij)k=i(jk)$。

以上几个等式由乘法表可以直接看出．所以，**H** 是结合代数，称为四元数代数，其元素称为四元数。四元数代数是19世纪中叶哈米尔顿（Hamilton）首先发现的注。

四元数 $\bar{\alpha}=a-bi-cj-dk$ 称为 $\alpha=a+bi+cj+dk$ 的共轭数。

引理1 在 **H** 中

$$\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}, \tag{1}$$

$$\overline{\alpha\beta}=\bar{\beta}\bar{\alpha}, \tag{2}$$

$$\alpha\bar{\alpha}=\bar{\alpha}\alpha=a^2+b^2+c^2+d^2. \tag{3}$$

证明留作练习。

$\alpha\bar{\alpha}$ 称为 α 的范数，记为 $N(\alpha)$．所以 $\alpha=0$ 当且仅当其范数为0．

H 是可除代数。事实上，设 $\alpha\neq0$，β 是两个任意的四元数，方程

$$\alpha\xi=\beta$$

显然有解 $\xi=\dfrac{1}{N(\alpha)}\bar{\alpha}\beta$，设另有解 ξ_1，则有

$$\alpha(\xi_1-\xi)=0,\quad \bar{\alpha}\alpha(\xi_1-\xi)=0.$$

因而 $N(\alpha)(\xi_1-\xi)=0$，$\xi_1=\xi$。

同理可证方程 $\xi\alpha=\beta$ 也有唯一解。

总之，可得

注 W. R. Hamilton(1805—1865)，爱尔兰数学家。

定理1 $\boldsymbol{H}$ 是 $\boldsymbol{R}$ 上不可换的四次可除结合代数。

二、弗洛比尼乌斯（Frobenius）定理[注]

$\boldsymbol{H}$、$\boldsymbol{C}$、$\boldsymbol{R}$ 都是 $\boldsymbol{R}$ 上的可除结合代数，次数分别为4、2、1，那末 $\boldsymbol{R}$ 上有没有其他可除结合代数呢？弗洛比尼乌斯定理回答了这个问题：

定理2 $\boldsymbol{H}$、$\boldsymbol{C}$ 和 $\boldsymbol{R}$ 是 $\boldsymbol{R}$ 上仅有的有限次可除结合代数。

为证本定理，先证

引理2 设 A 是 $\boldsymbol{R}$ 上的 n 次可除结合代数，则 $A\backslash\boldsymbol{R}$ 的元素都是 $\boldsymbol{R}$ 上的二次代数元.

证明：设 $\alpha\in A\backslash\boldsymbol{R}$，那末，$A$ 中 $n+1$ 个元素：$1,\alpha,\cdots,\alpha^n$ 线性相关，即存在不全为零的实数 a_0，a_1，…，a_n，适合

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0,$$

即 α 是实多项式

$$f(x)=a_0+a_1x+\cdots+a_nx^n$$

的根。而 $\boldsymbol{R}$ 上的多项式总可分解为一次或二次多项式之积，由于 A 是可除的，所以没有零因子，α 一定是某个一次或二次多项式的根。α 不能是一次多项式的根，否则推出 $\alpha\in\boldsymbol{R}$，因而 α 是某二次既约多项式 x^2+px+q 的根，即 α 是 $\boldsymbol{R}$ 上的二次代数元。

证毕

定理2的证明：设 A 是 $\boldsymbol{R}$ 上的 n 次可除结合代数，分三种情况讨论：

注 G. Frobenius(1849—1917)，德国数学家。

（1）$n=1$。这时 $A=\boldsymbol{R}$，A 是实数域。

（2）$n=2$。这时在 A 中存在 $\alpha\overline{\in}\boldsymbol{R}$，$\{1,\alpha\}$ 是 A 的一组基，假定 $\alpha^2=p\alpha+q$，则 α 是 $f(x)=x^2-px-q$ 的根，$f(x)$ 是 $\boldsymbol{R}$ 上的既约多项式。因而 $p^2+4q<0$。令 $p^2+4q=-r^2(r\in\boldsymbol{R})$，$i=\frac{1}{r}(2\alpha-p)\in A$，则 $i^2=\frac{1}{r^2}(4\alpha^2-4p\alpha+p^2)=\frac{1}{r^2}\cdot[4(\alpha^2-p\alpha-q)+4q+p^2]=\frac{p^2+4q}{r^2}=-\frac{r^2}{r^2}=-1$。即 i 是多项式 x^2+1 的根。显然 $\boldsymbol{R}(i)$ 是 $\boldsymbol{R}$ 的二次扩域，所以 $A=\boldsymbol{R}(i)$。

（3）$n>2$。这时由情况 2，A 一定包含多项式 x^2+1 的根 i。但 $\boldsymbol{R}(i)\subseteq A$，$\boldsymbol{R}(i)\neq A$（否则 A 将是 $\boldsymbol{R}$ 上的二次可除代数），故在 A 中存在 $\beta\overline{\in}\boldsymbol{R}(i)$。按照情况 2 的方法，又可得元素 j_1，适合 $j_1^2=-1$。$i+j_1\overline{\in}\boldsymbol{R}$，否则 $j_1\in\boldsymbol{R}(i)$，$\beta\in\boldsymbol{R}(i)$。同理，$i-j_1\overline{\in}\boldsymbol{R}$。根据引理 2，$i+j_1$ 和 $i-j_1$ 都是 $\boldsymbol{R}$ 上的二次代数元。设对应的 $\boldsymbol{R}$ 上的既约多项式为

$$x^2+ax+b \text{ 和 } x^2+cx+d,$$

那末，

$$(i+j_1)^2=-a(i+j_1)-b, \tag{4}$$

$$(i-j_1)^2=-c(i-j_1)-d. \tag{5}$$

而

$$(i+j_1)^2=-2+ij_1+j_1i, \tag{6}$$

$$(i-j_1)^2=-2-ij_1-j_1i, \tag{7}$$

因而，

$$-4=(i+j_1)^2+(i-j_1)^2=(-a-c)i+(-a+c)j_1+(-b-d),$$

$$(-a-c)i+(-a+c)j_1+(4-b-d)=0,$$

由于 $j_1 \overline{\in} \boldsymbol{R}(i)$，故 i，j_1，1 线性无关，因而 $a+c=0$，$-a+c=0$，即 $a=c=0$．由(4)式，$(i+j_1)^2=-b$，由(6)式，$ij_1+j_1i=-b+2$。

现在令 $t=-\frac{b}{2}+1\in\boldsymbol{R}$，则 $ij_1+j_1i=2t$。设 $j_2=j_1+ti$。因为 1，j_1，i 线性无关，故 $j_2 \overline{\in} \boldsymbol{R}$。而

$$
\begin{aligned}
j_2^2&=(j_1+ti)^2=j_1^2+tj_1i+tij_1+(ti)^2\\
&=-1-t^2+t(j_1i+ij_1)\\
&=-1-t^2+2t^2=-1+t^2\in\boldsymbol{R}.
\end{aligned}
$$

设 $j_2^2=-s^2(s\in\boldsymbol{R}^*)$，则 $-1+t^2=-s^2$。再设 $j=\frac{1}{s}j_2$，这时 $j^2=-1$，且

$$
\begin{aligned}
ij+ji&=\frac{1}{s}(ij_2+j_2i)=\frac{1}{s}[i(j_1+ti)+(j_1+ti)i]\\
&=\frac{1}{s}(ij_1+j_1i-2t)=0.
\end{aligned}
$$

因而 $ij=-ji$。令 $k=ij$，于是

$$k^2=(ij)(ij)=-(ij)(ji)=i^2=-1.$$

1，i，j，k 线性无关，否则可表 $k=a_1+b_1i+c_1j$ $(a_1, b_1, c_1\in\boldsymbol{R})$，用 i 左乘这一等式，得 $ik=a_1i-b_1+c_1k=a_1i-b_1+c_1(a_1+b_1i+c_1j)$。而 $ik=iij=-j$，所以

$$(c_1a-b_1)+(a_1+b_1c_1)i+(c_1^2+1)j=0.$$

因而 $c_1^2+1=0$（因为 1，i，j 线性无关），与 c_1 是实数矛盾。

1，i，j，k 的运算表显然与四元数的运算表一致（如 $jk=jij=-ijj=i$，等）。

在 A 中取形如 $a+bi+cj+dk(a, b, c, d\in\boldsymbol{R})$ 的一切元素组成的集合为 A_1，A_1 同构于四元数代数 $\boldsymbol{H}$。下面证明 $A_1=A$。否则，利用情况(2)的方法，可得 $l\in A$，$l \overline{\in} A_1$，适

合 $l^2=-1$，l 与 1，i，j，k 线性无关。利用与上述同样的方法(把 j_1 换为 l)，可得

$$il+li=a\in\boldsymbol{R}.$$

同理 $jl+lj=b\in\boldsymbol{R}$，$kl+lk=c\in\boldsymbol{R}$。故

$$\begin{aligned}lk&=(li)j=aj-i(lj)=aj-bi+(ij)l\\&=aj-bi+kl=aj-bi+c-lk.\end{aligned}$$

$$2lk=aj-bi+c.$$

用 k 右乘上式，得 $-2l=ai+bj+ck$，说明 l 与 1，i，j，k 线性相关，矛盾。所以 $A_1=A$。

即 $\boldsymbol{R}$ 上高于 2 次的有限次可除结合代数只有$\boldsymbol{H}$。

习　题　6·3

1. 求证在 $\boldsymbol{H}$ 中 $N(\alpha\beta)=N(\alpha)N(\beta)$。
2. 写出 $\boldsymbol{H}$ 在 $M_4(\boldsymbol{R})$中的正则表示。
3. 在 $\boldsymbol{H}$ 中求 $1+i-j+k$ 的逆元。
4. 求证 $\boldsymbol{H}$ 的中心是 $\boldsymbol{R}$。
5. 求证引理 1.
6. 在 $\boldsymbol{H}$ 中解方程：$(1+j)x=2+i-k$。
7. 在 $\boldsymbol{H}$ 中，若 α 是方程 $x^2+a_0x+b_0=0$ 的解，求证对于任意 $q\in\boldsymbol{H}$，$q\neq0$，$q^{-1}\alpha q$ 也是解。这里 a_0，$b_0\in\boldsymbol{R}$。

*§6·4　非结合代数简介

代数中乘法适合结合律时，就是结合代数，但常有许多代数是非结合的，这一节简要介绍三种常见的非结合代数：交错代数、李(Lie)代数、约当(Jordan)代数。

一、交错代数

定义1 设A为域F上的代数，对于任意$a, b \in A$，有

$$(a a)b = a(a b), \quad (b a)a = b(a a). \tag{1}$$

则称A为域F上的交错代数.

(1)式类似于结合律，但较弱，所以结合代数是交错代数的特例注. 下面介绍交错代数的重要例子——凯莱(Cayley)代数.

设$\boldsymbol{O}$是一切形如$\alpha+\beta e$的元素组成的集合，其中$\alpha, \beta \in \boldsymbol{H}$(四元数代数)，$e$代表一个新的符号. 如果$\beta=0$，则$\alpha+\beta e$记为$\alpha$，而$\alpha=0$时，记为$\beta e$. 在$\boldsymbol{O}$中规定

(1) $\alpha+\beta e=0$当且仅当$\alpha=\beta=0$；

(2) $(\alpha_1+\beta_1 e)+(\alpha_2+\beta_2 e)=(\alpha_1+\alpha_2)+(\beta_1+\beta_2)e$；

(3) $a(\alpha+\beta e)=(a\alpha)+(a\beta)e$，$(a\in \boldsymbol{R})$；

(4) $(\alpha_1+\beta_1 e)(\alpha_2+\beta_2 e)=(\alpha_1\alpha_2-\bar{\beta}_2\beta_1)+(\beta_2\alpha_1+\beta_1\bar{\alpha}_2)e$，

其中$\bar{\alpha}_2$，$\bar{\beta}_2$是α_2, β_2在$\boldsymbol{H}$中的共轭数.

易见，$\boldsymbol{O}$中元素的形式$\alpha+\beta e$中加和乘都与$\boldsymbol{O}$中的运算一致，如βe看作$(\beta+0e)(0+1e)$依照法则(4)，等于βe.

容易验证加法交换律、结合律成立，$0=0+0e$为零元，$-\alpha+(-\beta)e$是$\alpha+\beta e$的负元，所以$\langle \boldsymbol{O}, +\rangle$作成加群. 又由法则(3)，可知上述加群是$\boldsymbol{R}$上的向量空间，由法则(4)，$\langle \boldsymbol{O}, \cdot\rangle$是群胚. 乘法关于加法的分配律也是成立的. 此外，显然

$$k[(\alpha_1+\beta_1 e)(\alpha_2+\beta_2 e)]=[k(\alpha_1+\beta_1 e)](\alpha_2+\beta_2 e)$$
$$=(\alpha_1+\beta_1 e)[k(\alpha_2+\beta_2 e)], \quad (k\in \boldsymbol{R})$$

注　可以证明交错代数中任意两个元素生成的子代数是结合代数.

所以，$\boldsymbol{O}$ 为 $\boldsymbol{R}$ 上的代数，这个代数是非结合的，如 $(ij)e = ke \neq -ke = i(je)$.

显然 $\boldsymbol{H}$ 是 $\boldsymbol{O}$ 的子代数，所以 $\boldsymbol{O}$ 也是不可换代数.

$$1,\ i,\ j,\ k,\ e,\ ie,\ je,\ ke, \tag{2}$$

是 $\boldsymbol{O}$ 的一组基. 事实上，如果

$$a_1 + a_2 i + a_3 j + a_4 k + a_5 e + a_6 ie + a_7 je + a_8 ke = 0,$$

其中 $a_i \in \boldsymbol{R}$，则

$$(a_1 + a_2 i + a_3 j + a_4 k) + (a_5 + a_6 i + a_7 j + a_8 k)e = 0,$$

根据法则 1，$a_1 + a_2 i + a_3 j + a_4 k = 0$，$a_5 + a_6 i + a_7 j + a_8 k = 0$. 因而各 $a_i = 0$.

另外，对于任意的 $\alpha + \beta e = (a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)e \in \boldsymbol{O}$，有

$$\alpha + \beta e = a_1 + b_1 i + c_1 j + d_1 k + a_2 e + b_2 ie + c_2 je + d_2 ke,$$

即可表为元素(2)的线性组合. 于是，我们得到

定理 1 $\boldsymbol{O}$ 是 $\boldsymbol{R}$ 上包含 $\boldsymbol{H}$ 的八次不可换非结合代数.

$\boldsymbol{O}$ 称为凯莱代数，也称八元数代数.

$1 = 1 + 0e$ 是 $\boldsymbol{O}$ 的单位元.

定理 2 $\boldsymbol{O}$ 是 $\boldsymbol{R}$ 上的可除交错代数.

证明： 任取 $\alpha_1 + \beta_1 e$，$\alpha_2 + \beta_2 e \in \boldsymbol{O}$，由(4)可证

$$[(\alpha_1 + \beta_1 e)(\alpha_1 + \beta_1 e)](\alpha_2 + \beta_2 e)$$
$$= (\alpha_1 + \beta_1 e)[(\alpha_1 + \beta_1 e)(\alpha_2 + \beta_2 e)],$$
$$[(\alpha_2 + \beta_2 e)(\alpha_1 + \beta_1 e)](\alpha_1 + \beta_1 e)$$
$$= (\alpha_2 + \beta_2 e)[(\alpha_1 + \beta_1 e)(\alpha_1 + \beta_1 e)].$$

在 $\boldsymbol{O}$ 中规定 $\alpha + \beta e$ 的范数为非负数

$$n(\alpha + \beta e) = N(\alpha) + N(\beta),$$

其中 $N(\alpha)$ 表示 α 在 $\boldsymbol{H}$ 中的范数. 显然仅当 $\alpha + \beta e = 0$ 时，范

数为 0，且

$$n((\alpha+\beta e)(\gamma+\delta e))=n(\alpha+\beta e)n(\gamma+\delta e).$$

设已知 **O** 中元素 $\xi=\alpha+\beta e\neq 0$ 和 $\eta=\gamma+\delta e$，不难验证方程 $\xi\zeta=\eta$ 有解 $\zeta=\frac{1}{n(\xi)}[\bar{\alpha}\gamma+\bar{\delta}\beta)+(\delta\bar{\alpha}-\beta\bar{\gamma})e]$.

假若还有一解 ζ_1，则 $\xi\zeta=\xi\zeta_1$，即

$$\xi(\zeta-\zeta_1)=0,\quad n(\xi)n(\zeta-\zeta_1)=0.$$

由于 $\xi\neq 0$，$n(\xi)\neq 0$，故 $n(\zeta-\zeta_1)=0$，$\zeta=\zeta_1$.

同样可证方程 $\zeta\xi=\eta$ 也有唯一解.

证毕

O 是 **R** 上的有限次可除交错代数，那末有没有其他次数的可除交错代数呢?

定理 3 **O** 是 **R** 上唯一的有限次可除交错（但非结合）代数.

因而可知 **R** 上的有限次可除交错代数只有四个，即 **R**(1 次)、**C**(2 次)、**H**(4 次)、**O**(8 次)。这个结论常称为推广的弗洛比尼乌斯定理(证明从略).

二、李代数[注]

定义 2 设 L 是域 F 上的代数，其积记为 $[a,b]$. 如果对于任意的 $a,b,c\in L$，有

(1) $[a,b]=-[b,a]$;

(2) $[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0$,

则称 L 为域 F 上的李代数.

注 S. Lie(1842—1899)挪威数学家，李群与李代数的创始人.

李代数中，总有$[a,a]=-[a,a]$，即当F的特征$\neq 2$时$[a,a]=0$。

例1 $\boldsymbol{R}_3$关于向量积和向量加法与数乘作成$\boldsymbol{R}$上的李代数。

证明：设e_1，e_2，e_3是$\boldsymbol{R}_3$的一组基。$\boldsymbol{R}_3$的任意元素可写成

$$\alpha=a_1e_1+a_2e_2+a_3e_3.$$

设$\beta=b_1e_1+b_2e_2+b_3e_3$，由向量代数知识知道，

$$[\alpha,\beta]=(a_2b_3-b_3a_2)e_1+(a_3b_1-a_1b_3)e_2$$
$$+(a_1b_2-a_2b_1)e_3.$$

不难验证，向量积关于向量加法适合分配律，而且对于$k\in\boldsymbol{R}$，有

$$k[\alpha,\beta]=[k\alpha,\beta]=[\alpha,k\beta].$$

同时，定义2中的两个等式也均成立。由于$\boldsymbol{R}_3$关于加法与数乘是向量空间，所以$\boldsymbol{R}_3$作成$\boldsymbol{R}$上的李代数。

任何结合代数可以改换为李代数，即

例2 设A为F上的结合代数。如果乘法改为$[a,b]=ab-ba$，则A关于新的乘法作成李代数，记为A^-。

证明：任取a，b，$c\in A$，则

$$[a,b]=ab-ba=-(ba-ab)=-[b,a],$$

$$[a,[b,c]]+[b,[c,a]]+[c,[a,b]]$$
$$=a[b,c]-[b,c]a+b[c,a]-[c,a]b$$
$$+c[a,b]-[a,b]c$$
$$=abc-acb-bca+cba+bca-bac-cab+acb$$
$$+cab-cba-abc+bac$$
$$=0.$$

下面证明分配律：

$$[a,b+c]=a(b+c)-(b+c)a=ab+ac-ba-ca$$
$$=[a,b]+[a,c].$$

同理 $[b+c,a,]=[b,a]+[c,a]$.

另外，对于$k\in F$，有

$$k[a,b]=k(ab-ba)=k(ab)-k(ba)$$
$$=(ka)b-b(ka)=[ka,b].$$

同理$k[a,b]=[a,kb]$．因而§6·1的(1)式成立．至于A^-的向量空间结构并未变化，所以A^-作成F上的李代数．

另一方面，任给一个李代数L，都有同一域上的结合代数A，使L同构于A^-的子代数.这是毕克豪夫—魏特(Birkhoff-Witt)定理，在此就不证明了．

三、约当代数注

定义 3 设J是特征$\neq 2$的域F上的代数，对于任意的$a,b\in J$，有

(1) $a\cdot b=b\cdot a$;

(2) $a^2\cdot(b\cdot a)=(a^2\cdot b)\cdot a$, $(a^2=a\cdot a)$

则称J为F上的约当代数.

任何约当代数是可换代数，不一定是结合代数，因为定义中的条件(2)比结合律弱．所以可换的结合代数是约当代数．有趣的是，如同李代数那里一样，任意结合代数都可以改换成约当代数：

例 3 设A为域F上的结合代数．将A中乘法改为$a\cdot b$

注 约当代数由德国物理学家 P. Jordan(与代数中常提到的C. Jordan并非一个人)在1933年创立，由阿尔贝脱(A. Albert)命名.

$=\frac{1}{2}(ab+ba)$，则作成 F 上的约当代数，记为 A^+。此处假定 F 的特征 $\neq 2$。

注意：在这里 $\frac{1}{2}$ 理解为 $(2\cdot 1)^{-1}$，1 是 F 的单位元，F 的特征 $\neq 2$，故 $\frac{1}{2}$ 有意义。

A^+ 与 A 的向量空间相同，只须验证分配律及 §6·1（1）式和定义 3 中的两个条件（作为练习）。

在约当代数中，规定元素的方幂

$$a^1=a,\quad a^k=a^{k-1}\cdot a,\ (k\geqslant 2)$$

则可以验证

$$a^k\cdot a^l=a^{k+l}.$$

这一性质称为幂结合律。由此可以推知约当代数中任意一个元素生成的子代数是结合代数。前面说过，交错代数中任意两个元素生成的子代数是结合代数，所以交错代数比约当代数有更强的"结合性"。

*§6·5 模

模可以看作环与群共同产生的代数系，它是向量空间的推广。

定义 1 设 R 是有单位元的环，M 是可换群。如果有 $R\times M$ 到 M 的映射（称为外乘法）$(r,m)\to rm$，满足以下条件：

（1）$r(m_1+m_2)=rm_1+rm_2$；

（2）$(r_1+r_2)m=r_1m+r_2m$；

(3) $(rs)m=r(sm)$;

(4) $1m=m$。

其中 $r_1, r_2, r, s\in R$, $m, m_1, m_2\in M$, 1是R的单位元. 这时，称M为左R——模，简称R——模.

如果把定义中的外乘法因子次序颠倒，则不难得到右R——模的概念.

例 1 设R是域F，则F——模是F上的向量空间.

例 2 任意可换群G可看作$\mathbf{Z}$——模，因为规定$na=a^n$ $(a\in G,\ n\in\mathbf{Z})$显然适合定义1中的条件.

例 3 设I为环R的理想，对于$a\in I$，$r\in R$，ra规定为R中的乘法，则显然$\langle I,+\rangle$可以看作R——模.

我们可以按照通常的方法定义子模、商模、模同态、模同构、模的直和以及子模的生成系. 如果一个R——模M的生成系只含一个元素a，则称为R——循环模，即这时

$$M=\langle a\rangle=\{ra\,|\,r\in R\}.$$

以下介绍一类重要模的结构定理：

定理 1（有限生成模基本结构定理） 设D是主理想环，$M(\neq 0)$是有限生成的D——模(即生成系只含有限个元素)，则M同构于有限个循环子D——模的直和.

证明从略.

当$D=\mathbf{Z}$时，循环D——子模是循环子群，由定理1可推知：有限生成的可换群同构于有限个循环子群的直和. 这是我们在群论中已有的结果(见§3·12定理7).

当$D=F$(域)时，有限生成的F——模是F上的有限维空间，F——循环模是一维子空间. 这时，定理1可以得知：有限维向量空间同构于有限个一维子空间的直和. 这是线性

代数中熟知的结果。

本 章 提 要

一、代数的定义：域F上的向量空间A如果有乘法运算，对加法适合分配律，且满足§6·1中(1)式，则称A为F上的代数。按乘法的特殊性质，又有结合代数、可换代数、可除代数等类型。基元素的运算性质，将决定代数的相应性质。

二、子代数、理想、商代数、同态、同构是刻划代数内部结构及代数之间关系的重要概念，其定义类似于群、环等代数系的相应概念。

三、正则矩阵表示：n次结合代数同构于n阶方阵代数的一个子代数。

四、弗洛比尼乌斯定理：$\boldsymbol{H}$、$\boldsymbol{C}$和$\boldsymbol{R}$是$\boldsymbol{R}$上仅有的有限次可除结合代数。

复 习 题 六

1. 求证：有单位元的二次代数是可换代数。

2. 设$G=\{1,-1,i,-i\}$，G是乘群，$\boldsymbol{C}$是否为G在$\boldsymbol{R}$上的群代数？

3. 求证：代数A的中心C在任意自同构下的象集仍为C。

4. 设A是域F上的向量空间，在A中规定任意两元素之积为0，求证这时A作成F上的代数(称为零代数)。

5. 求证：零代数的任意子空间也是子代数和理想。

6. 根据习题 6·2 第 3 题的结果，求证：$F[x]/F_0[x] \cong F$。

7. 在 $\boldsymbol{H}$ 中，取 $G=\{1,-1,i,-i,j,-j,k,-k\}$。求证：$\langle G,\cdot\rangle$ 是群（称为四元数群）。写出 G 的所有子群。G 是否同构于 C_8 或 D_4？

8. 求证：可换代数的全体幂零元（即对某个 n，$a^n=0$ 的元素 a）作成理想。

9. 在结合代数中，求证：若 ab 为幂零元，则 ba 为幂零元。

*10. 设域 F 上的结合代数 A 有单位元 $e\neq 0$。求证：A 的中心含有子域 F_1 同构于 F。

*11. 求证：有限次无零因子代数 R 是可除代数。

12. 求证：复数域上的有限次可除结合代数只有复数域本身。

13. 在 $\boldsymbol{H}$ 中，规定 $\alpha=a_0+a_1i+a_2j+a_3k$ 的迹 $T(\alpha)=2a_0$，求证 α 适合二次方程

$$x^2-T(\alpha)x+N(\alpha)=0.$$

第七章 格

本章介绍格论的初步知识．格论源于许多数学分支，近代格论形成于本世纪三十年代，现在已成为代数的重要组成部分，并在泛函分析、赋值论、几何、逻辑、计算机科学、图论等方面有着广泛的应用．

§7·1 半 序 集

半序集是相对于全序集而言的．

一、全序集

先看一个例子．在整数集 $\mathbf{Z}$ 中，$\leqslant$显然有以下四条性质：

（1）反身性：对于任意的 $a\in\mathbf{Z}$，有 $a\leqslant a$；

（2）反对称性：如果 $a\leqslant b$，$b\leqslant a$，则 $a=b$；

（3）传递性：如果 $a\leqslant b$，$b\leqslant c$，则 $a\leqslant c$；

（4）可比较性：对于任意的 $a,b\in\mathbf{Z}$，$a\leqslant b$ 和 $b\leqslant a$ 至少有一成立．

同样可知，$\mathbf{Z}$ 关于$\geqslant$也有以上性质．

定义 1 集合 A 中设有关系 R．如果 R 具有反身性、反对称性、传递性、可比较性，则称为集合 A 的全序关系．这时，称 A 关于 R 构成全序集或链，记为 $\langle A,R\rangle$．

所以，$\langle\mathbf{Z},\leqslant\rangle$和$\langle\mathbf{Z},\geqslant\rangle$都是全序集．同样可知 $\langle\mathbf{R},\leqslant\rangle$

和$\langle \mathbf{R}, \geqslant \rangle$也都是全序集。

显然全序集的非空子集也是全序集。

$\mathbf{Z}$ 中的整除关系不是全序关系，因为尽管反身性和传递性都具备，但不适合反对称性和可比较性。如 $2|-2$，$-2|2$，但 $2\neq-2$；$2\nmid 3$，$3\nmid 2$，2 和 3 不可比较。

复数集 $\mathbf{C}$ 中如果引进以下关系：$a+bi\leqslant c+di$ 当且仅当 $a\leqslant c$ 且 $b\leqslant d$，则易见反身性、反对称性、传递性都适合，但可比较性不适合，如 $1+0i$ 和 $0+i$ 既不适合 $1+0i\leqslant 0+i$，也不适合 $0+i\leqslant 1+0i$。

二、半序集

定义 2 集合 A 中的关系 $\mathbf{R}$，如果具有反身性、反对称性、传递性，则称为集合 A 的半序关系。这时，称 A 关于 R 构成半序集，记为$\langle A, R\rangle$。

显然全序集是半序集。上述$\langle \mathbf{C}, \leqslant \rangle$是半序集。整除关系是正整数集 $\mathbf{P}$ 的半序关系，事实上，任取 $a\in \mathbf{P}$，则 $a|a$；如果 $a|b$，$b|a$，则 $a=b$；如果 $a|b$，$b|c$，则 $a|c$。

同一个集合关于不同的半序关系作成的半序集，应认为是不同的半序集。如 $\mathbf{P}$ 关于通常的$\leqslant$也作成半序集。应认为$\langle \mathbf{P}, \leqslant \rangle$和$\langle \mathbf{P}, | \rangle$是不同的半序集。

例 1 设 S 是任意非空集。在 S 中的所有子集构成的子集族 $F(S)$中，$\subseteq$显然是半序关系，即$\langle F(S), \subseteq \rangle$是半序集。

例 2 设 G 是群，L 是 G 中所有子群组成的集合，子群的包含关系是 L 的半序关系。

任意集合都可以引进以下平凡半序关系：

例 3 任意集合 A 中，相等是半序关系，因为自身性、

反对称性、传递性显然成立。

例 4 $\boldsymbol{Z}$ 中通常的$<$不是半序关系，因为不适合反身性，如 $2 \not< 2$。

例 5 实多项式集 $\boldsymbol{R}[x]$中的整除关系不是半序关系，因为不适合反对称性，如 $x^2-1|2x^2-2$，$2x^2-2|x^2-1$，但 $x^2-1\neq 2x^2-2$。

例 6 $\boldsymbol{R}$ 中规定 aRb 当且仅当 $a\leqslant b$ 且 $b-a<1$。则 R 不是 $\boldsymbol{R}$ 的半序关系，因为 $1\ R\ 1.7$，$1.7\ R\ 2.5$，但 $1\ \bar{R}\ 2.5$，传递性不适合。

今后，约定凡半序关系除已有特定记号外，通常用$\leqslant$表示，读作"小于等于"(不要狭义地理解为数的小于等于)。如果 $a\leqslant b$，$a\neq b$，则记之 $a<b$，读作 a "小于"b。

显然半序集的子集也是半序集。

半序集可以有一个全序子集，其全序关系是半序集的半序关系。如$\langle \boldsymbol{C},\leqslant\rangle$中，全体实数构成全序子集$\langle \boldsymbol{R},\leqslant\rangle$。

三、覆盖与覆盖图

定义 3 在半序集$\langle A,\leqslant\rangle$中，如果 $a<b$，且不存在 $c\in A$，使 $a<c<b$，则称 b 覆盖 a。

如$\langle \boldsymbol{Z},\leqslant\rangle$中，2 覆盖 1，3 覆盖 2 等。

在半序集中，任意一对元素 a 和 b，b 是否覆盖 a 是完全确定的，所以覆盖是半序集中由$\leqslant$生成的一个新的关系。

例 7 设 $A=\{a,b,c,d,e\}$，规定对每个 $x\in A$，$x\leqslant x$；此外，$a\leqslant c$，$b\leqslant c$，$c\leqslant d$，$c\leqslant e$，$a\leqslant d$，$a\leqslant e$，$b\leqslant d$，$b\leqslant e$。求证$\langle A,\leqslant\rangle$是半序集。写出$\langle A,\leqslant\rangle$的覆盖元素对。

解： 由已知，反身性成立。如果反对称性不成立，必有

一对元素 x，y，满足 $x\leqslant y$，$y\leqslant x$，但 $x\neq y$。A 中没有这样元素。此外传递性显然成立，所以 $\langle A,\leqslant\rangle$ 是半序集。易见，c 覆盖 a 和 b，d 和 e 覆盖 c。

覆盖关系也可能是空关系，即任意两个元素都互不覆盖。如 $\langle \mathbf{R},\leqslant\rangle$ 中，对任意 a，b，如果 $a<b$，则有 $a<\frac{a+b}{2}<b$，所以没有覆盖 a 的元素。

定义 4 在半序集中，如果 a_1 覆盖 a_0，a_2 覆盖 $a_1,\cdots,a_n$ 覆盖 a_{n-1}，则称 $\{a_0, a_1, \cdots, a_n\}$ 是一个覆盖链。n 称为链长。

在有限半序集中，$<$ 关系可以通过覆盖链实现，这就是

定理 1 设 $\langle A,\leqslant\rangle$ 是有限半序集。$a<b$ 的充要条件是有起于 a 终于 b 的覆盖链。

证明：如果 b 不覆盖 a，则有 $c\in A$，使 $a<c<b$。如果上式相邻元素不是覆盖元素对，可以继续插入新元素。由于 A 有限，最后必然得到一系列元素，适合

$$a<a_1<a_2<\cdots<a_n=b. \tag{1}$$

这里每个元素覆盖前一个元素，得到一个覆盖链。

反之，如果有覆盖链起于 a，终于 b，由传递性，必然 $a<b$。

证毕

对于有限半序集，可以用图表示覆盖关系，这就是所谓覆盖图或哈级(Hasse)图。

在平面上用圆点表示半序集的元素，如果 b 覆盖 a，就在 a 点的上方画上 b，并连以直线段。据定理 1，$a<b$ 当且仅当有一条上升的折线由 a 通向 b。例 7 的覆盖图如图 7—1.

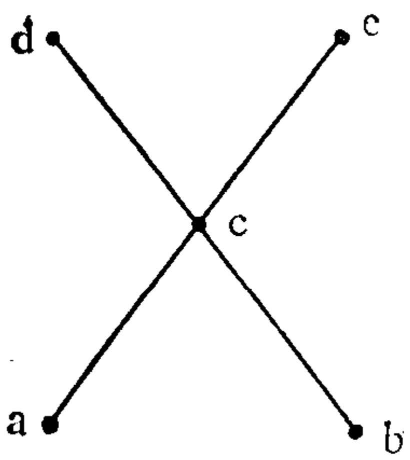


图 7—1

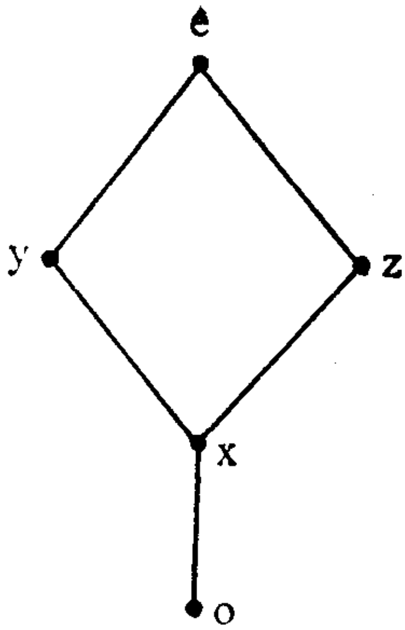


图 7—2

反之，由覆盖图也可以决定元素的半序关系。反之，由覆盖图也可决定元素的半序关系.如图 7—2 所示：x 覆盖 o，y 覆盖 x，z 覆盖 x，e 覆盖 y，e 覆盖 z，容易验证 $\{o, x, y, z, e\}$ 作成半序集.

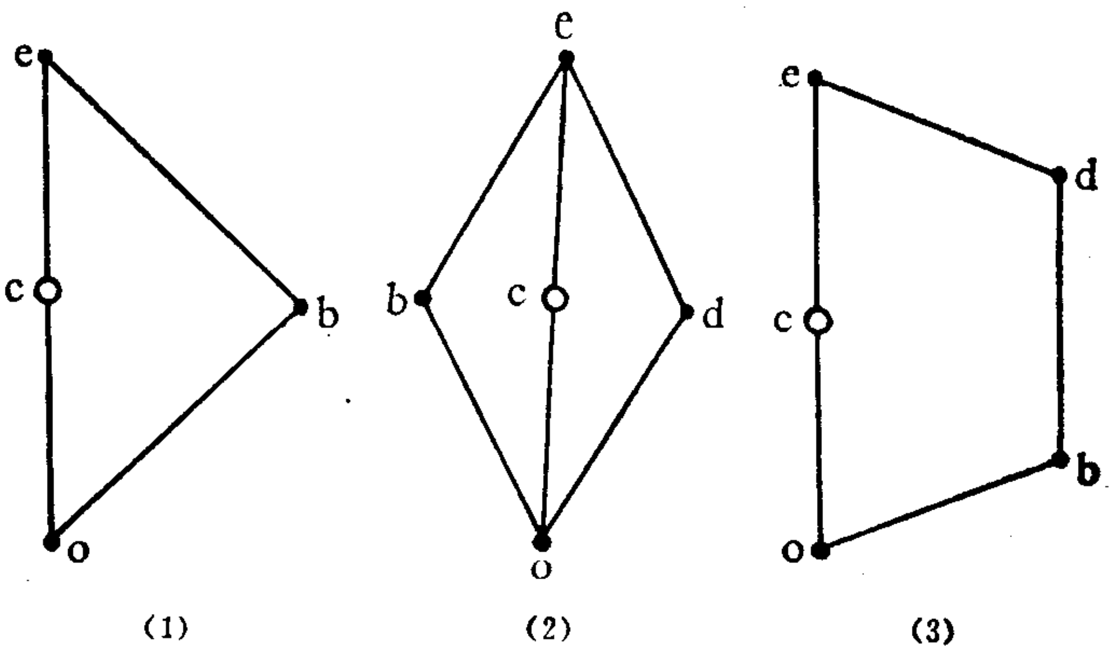


图 7—3

不过，并非所有图都能作成半序集的覆盖图。如图 7—3(1)(不包括空心点 c)，eo 有连线，说明 e 覆盖 o，但 eb 和 bo 也有连线，说明 $0<b$，$b<e$，$o<b<e$，这与 e 覆盖 o 矛盾。同样可知 7-3(2)、(3)图也不是覆盖图。但只要适当增加点，就可以作成覆盖图(图 7-3 中空心点 c 为新增点)。

四、半序集中的特殊元素

定义 5 设 a 是半序集 $\langle A,\leqslant\rangle$ 的元素，如果不存在元素 $b\in A$，使 $a<b$，则称 a 为 A 的一个极大元。如果不存在 $c\in A$，使 $c<a$，则称 a 为 A 的一个极小元。

如 $(F(S),\subseteq)$ 中，S 是极大元，ϕ 是极小元。$\langle \boldsymbol{C},\leqslant\rangle$ 中既无极大元也无极小元。

无极大元或极小元的半序集总是无限集，这因为我们有

定理 2 有限半序集 $\langle A,\leqslant\rangle$，总有极大元和极小元。

证明：设 $a\in A$，如果 a 不是极大元，则有 $b\in A$，使 $a<b$。如果 b 不是极大元，则有 $c\in A$，使 $b<c$。由于 A 有限，这一过程必然经有限次而中止，最后得元素 $m\in A$。显然 m 是一个极大元。同理，极小元也存在。

证毕

极大(小)元不一定唯一。如图 7—1 所示的例 7 中，d 和 e 都是极大元，a 和 b 都是极小元。

定义 6 设 e 和 o 是半序集 $\langle A,\leqslant\rangle$ 的元素，如果对于 $a\in A$ 都有 $a\leqslant e$，则称 e 是 $\langle A,\leqslant\rangle$ 的单位元。如果对于 $a\in A$，都有 $o\leqslant A$，则称 o 是 $\langle A,\leqslant\rangle$ 的零元。

如 $\langle F(S),\subseteq\rangle$ 中，S 是单位元，而 ϕ 是零元。

显然，单位元（零元）一定是极大（小）元。反之不然，

如例7中，极大元d,e不是单位元。

半序集如果有单位元，必唯一。事实上，设e_1，e_2是单位元，则$e_1 \leqslant e_2$，$e_2 \leqslant e_1$，由反对称性，$e_1 = e_2$。同理，零元也有同样性质。

另一方面，我们又有

定理3 有限半序集$\langle A, \leqslant\rangle$中，如果有唯一的极大元，则必是单位元；如果有唯一的极小元，则必是零元。

证明：如果$|A| = 1$，定理显然正确。现假定$|A| \neq 1$。设e是唯一的极大元，任取$a_1 \neq e$，由于a_1不是极大元，故有a_2，使$a_1 < a_2$，如果a_2不是极大元，又有a_3，使$a_2 < a_3, \cdots$。由于A有限，经有限次，得到链$a_1 < a_2 < \cdots < a_n$，其中a_n是一个极大元。既然极大元唯一，故$a_n = e$。因而$a_1 < e$，e是单位元。

同理可证第二个结论。

证毕

五、界与确界

半序集中还有一个常见的概念，这就是界。

定义7 设B是半序集$\langle A, \leqslant\rangle$的子集，$a \in A$，如果对于所有的$b \in B$，都有$b \leqslant a$，则称$a$为$B$的一个上界。如果对于任意的$b \in B$，都有$a \leqslant b$，则称$a$为$B$的一个下界。

例如，$A = \{1, 2, 3, 6, 8, 15, 16, 30, 210, 300\}$按整除关系作成半序集。取$B = \{3, 6, 15, 30\}$，则30，300，210都是$B$的上界(它们是$B$中数的公倍数)，3，1是$B$的下界(它们是$B$中数的公因数)。$A$的覆盖图如图7—4。

任意半序集$\langle A, \leqslant\rangle$的子集$B$的所有上界自然也是$A$的子

集，这个子集的零元如果存在，称为 B 的上确界，记为 $\sup B$。同样，B 的所有下界的集合的单位元若存在，则称为 B 的下确界，记为 $\inf B$。

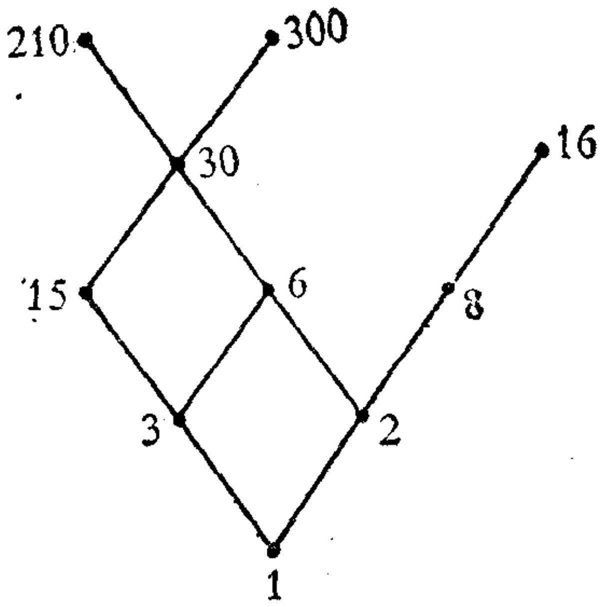


图 7—4

上例中，$\sup B=30$，$\inf B=3$。如取 $C=\{6,8,30\}$，则 C 只有下确界 2，没有上确界。半序集的子集的上(下)确界只要存在，一定唯一。

可以认为，上确界是最小上界，下确界是最大下界。

如设 B 为 $\langle C,\leqslant\rangle$ 中模不大于 1 的复数集合，则有 $\sup B=1+i$，$\inf B=-1-i$。事实上，任取 $b=u+vi\in B$，则 $u\leqslant1$，$v\leqslant1$，故 $b\leqslant1+i$；另一方面，设 $c=s+ti$ 是 B 的上界，则对于 $b=u+vi\in B$，有 $b\leqslant c$，特别 $0+i\leqslant s+ti$，$1+0i\leqslant s+ti$，即 $1\leqslant t$，$1\leqslant s$。所以 $1+i\leqslant s+ti=c$。因而 $1+i=\sup B$。同理，$\inf B=-1-i$。

习 题 7·1

1. 求证：任意有限集可以引进全序关系。并问有多少不同的全序关系？

2. 以下集合关于对应的关系是否作成全序集或半序集？

(1) 平面上的全体始于 o 的向量关于模的大小；

(2) 平面上的全体三角形关于面积大小；

(3) [0,1]上全体连续函数，规定 $f\leqslant g$ 为对于 $x\in[0,1]$ 有 $f(x)\leqslant g(x)$；

(4) 2^n阶的循环群的全体子群关于包含关系；

(5) {1，2，3，4，5}关于整除关系以及关于大小。

3．上题中半序集对应的单位元或零元（如果存在）是什么？

4．在半序集中，若有 $a_1\leqslant a_2\leqslant\cdots\leqslant a_n\leqslant a_1$，则必有 $a_1=a_2=\cdots=a_n$。证明之。

5．设有半序集的覆盖图（如图 7—5），试求所有极大元与极小元，并求：

$$\sup\{d,f\},\ \sup\{a,b,c\};$$
$$\inf\{g,h\},\ \inf\{i,f,e,c\}.$$

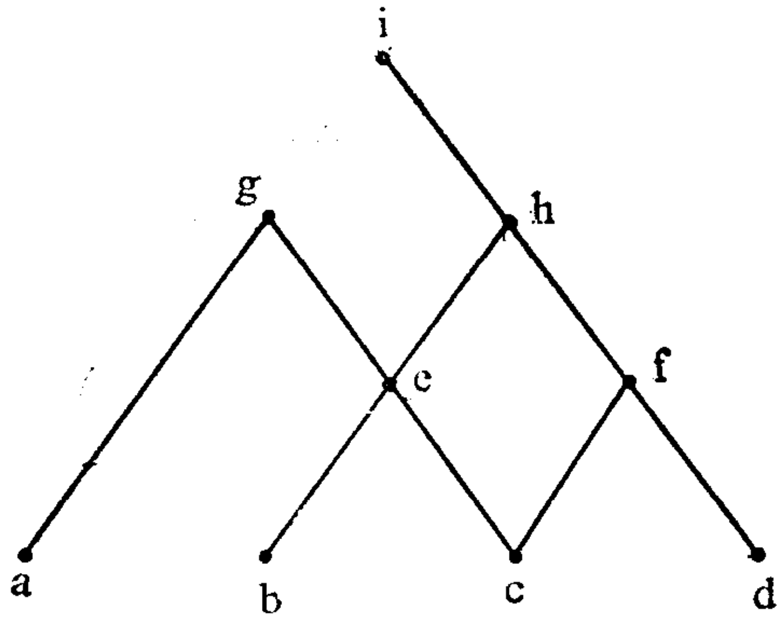


图 7—5

6．作出克来因四元群 B_4 子群关于包含关系的半序集的覆盖图。

7．一个群的所有正规子群按包含关系是否作成半序集？

为什么？

8．求证：全(半)序集的子集也是全(半)序集．

9．有单位元的半序集中，求证没有除单位外的极大元．叙述关于零元的相应性质．

§7·2 格的一般概念

上节看到，半序集中子集的上、下确界不一定存在，下面专门讨论一类重要的半序集——格．格的任意有限子集都存在上、下确界．

一、什么是格

定义1 设$\langle L,\leqslant\rangle$是半序集，如果对于任意的$a,b\in L$，$\sup\{a,b\}$和$\inf\{a,b\}$都存在，则称$\langle L,\leqslant\rangle$为格．

下面为了简便，用$a\vee b$表示$\sup\{a,b\}$，用$a\wedge b$表示$\inf\{a,b\}$．

显然，在格中，$a\leqslant b$等价于$a\vee b=b$，也等价于$a\wedge b=a$．

例1 求证：全序集是格．

证明：设a,b是全序集的两个元素，则$a\leqslant b$和$b\leqslant a$至少有一成立．若$a\leqslant b$，则$b=a\vee b$，$a=a\wedge b$．

例2 求证：$\langle \boldsymbol{C},\leqslant\rangle$是格．

证明：任取$a+bi$，$c+di\in \boldsymbol{C}$，显然

$$(a+bi)\vee(c+di)=\max\{a,c\}+i\max\{b,d\},$$

$$(a+bi)\wedge(c+di)=\min\{a,c\}+i\min\{b,d\}.$$

例3 求证：集合S的所有子集按包含关系作成的半序

集$\langle F(S), \subseteq\rangle$是格（称为子集格）。

证明：设$T_1, T_2 \subseteq S$，则显然

$$T_1 \vee T_2 = T_1 \cup T_2 \in F(S),$$

$$T_1 \wedge T_2 = T_1 \cap T_2 \in F(S).$$

例 4 求证：群G的所有子群按包含关系作成的半序集是格（称为子群格）。注

证明：设H_1, H_2是群G的子群。$H_1 \cup H_2$一般不是子群，考虑由$H_1 \cup H_2$生成的子群$\langle H_1 \cup H_2\rangle$，它包含$H_1$和$H_2$，同时任一包含$H_1$和$H_2$的子群也包含它，即$\langle H_1 \cup H_2\rangle$是$\{H_1, H_2\}$的上确界，$H_1 \vee H_2 = \langle H_1 \cup H_2\rangle$。此外，由于$H_1 \cap H_2$是子群，所以$H_1 \wedge H_2 = H_1 \cap H_2$。

例 5 求证：任意环R的所有理想按包含关系作成格（称为理想格）。

证明：设I和J是R的任意两个理想，I_1和I_2的并$I_1 \cup I_2$一般不再是理想，而$I_2 \cup I_2$生成的理想为$I_1 + I_2$，而它是包含I_1和I_2的最小理想，所以$I \vee I_2 = I_1 + I_2$。此外，显然$I_1 \wedge I_2 = I_1 \cap I_2$。

图 7—2、3、（包括 c 点）对应的半序集是格。图 7—1（例 7）对应的半序集不是格，如$\sup\{d, e\}$不存在。

二、格的充要条件

定理 1 在格$\langle L, \leqslant\rangle$中，成立：

(L_1) $a \vee a = a$，$a \wedge a = a$；（幂等律）

(L_2) $a \vee b = b \vee a, a \wedge b = b \wedge a$；（交换律）

注 反之，可以证明，任意格同构于某群的子群格。因而子群格类概括了所有的格。

(L_3) $a\vee(b\vee c)=(a\vee b)\vee c$,

$a\wedge(b\wedge c)=(a\wedge b)\wedge c$；（结合律）

(L_4) $a\vee(a\wedge b)=a$，$a\wedge(a\vee b)=a$；（吸收律）

证明：(L_1)，(L_2)显然成立．下面证(L_3)：$b\leqslant b\vee c\leqslant a\vee(b\vee c)$．同理$a$，$c$也以$a\vee(b\vee c)$为上界．因而$a\vee b\leqslant a\vee(b\vee c)$，$(a\vee b)\vee c\leqslant a\vee(b\vee c)$．同法可证$a\vee(b\vee c)\leqslant(a\vee b)\vee c$．($L_3$)第一式成立．同样可得第二式．再证($L_4$)：$a\wedge b\leqslant a$，$a\leqslant a$，故$a\vee(a\wedge b)\leqslant a$，但显然$a\leqslant a\vee(a\wedge b)$，故$a\vee(a\wedge b)=a$．同法可证第二式．

证毕

(L_1)～(L_4)反映了格的本质特性．反过来，如果集合L有两个代数运算，一个叫做$\vee$，一个叫做$\wedge$，并且它们适合性质(L_1)～(L_4)，那末L可以作成格，所以，有时直接用(L_1)～(L_4)作为格的定义，这就是

定理 2 假设在集合L中定义着两个代数运算：$\vee$和$\wedge$，它满足(L_1)，(L_2)，(L_3)，(L_4)，则L是一个格，且其上、下确界与$\vee$、$\wedge$一致．

分析：先在L中引入半序关系，再证明每两个元素有上、下确界，且与$\vee$、$\wedge$一致．

证明：对于任意一对元素a、b，规定当且仅当$a\vee b=b$时$a\leqslant b$．$\leqslant$是L的关系．下面验证$\leqslant$满足半序的三个条件：

对于任意的$a\in L$，由(L_1)，$a\vee a=a$，故$a\leqslant a$；如果$a\leqslant b$，$b\leqslant a$，则$a\vee b=b$，$b\vee a=a$，由(L_2)，$a\vee b=b\vee a$，故$a=b$；如果$a\leqslant b$，$b\leqslant c$，则$a\vee b=b$，$b\vee c=c$，$a\vee c=a\vee(b\vee c)=(a\vee b)\vee c=b\vee c=c$，$a\leqslant c$．

所以$\langle L,\leqslant\rangle$是半序集．

任取 a, $b\in L$, 由(L_3)和(L_1), $a\vee(a\vee b)=(a\vee a)\vee b=a\vee b$, 所以 $a\leqslant a\vee b$, 同理 $b\leqslant a\vee b$. 因而 $a\vee b$ 是 $\{a,b\}$ 的一个上界. 现在, 设 u 是 $\{a,b\}$ 的任一上界, 则 $a\leqslant u$, $b\leqslant u$, $a\vee u=u$, $b\vee u=u$, 由(L_3), 有 $(a\vee b)\vee u=a\vee(b\vee u)=a\vee u=u$. 故 $a\vee b\leqslant u$, $a\vee b=\sup\{a,b\}$. 同理 $a\wedge b=\inf\{a,b\}$.

总之, $\langle L,\leqslant\rangle$ 是格, 而且这里的 $\vee$ 和 $\wedge$ 两个代数运算正好与按 $\leqslant$ 的上确界和下确界意义一致.

证毕

三、完全格

格只保证任意两个元素(因而任意有限个元素)存在上确界和下确界, 不能保证无限子集有上确界和下确界. 现在对格的条件加以强化, 引进完全格的概念.

定义 2 如果格 L 的任意非空子集有上确界和下确界, 则称 L 为完全格.

完全格 L 的上确界即 L 的单位元, 下确界是 L 的零元, 因而可得

定理 3 完全格存在单位元和零元.

集合的子集格是完全格的最基本的例子. S 的任意子集族 $\{S_\lambda\mid\lambda\in\Lambda\}$ 的上确界是 $\bigcup\limits_{\lambda\in\Lambda}S_\lambda$, 下确界是 $\bigcap\limits_{\lambda\in\Lambda}S_\lambda$. 群的子群格, 环的理想格也是完全格(请读者试证).

$\langle \boldsymbol{R},\leqslant\rangle$ 和 $\langle \boldsymbol{C},\leqslant\rangle$ 等都不是完全格, 因为它们没有单位元和零元.

由于格中任意有限个元素总有上(下)确界, 所以有限

格总是完全格。

定理 4 半序集 L 是完全格的充要条件是存在单位元且任一非空子集存在下确界.

证明：必要性显然. 充分性只须证明 L 的每个非空子集有上确界. 设 $A\subseteq L$，$A\neq\phi$。考虑 A 的上界的集合 B. B 至少含 L 的单位元，故 $B\neq\phi$. 因 B 有下确界，设为 d. 下面证明 d 为 A 的上确界。事实上，如果 $a\in A$，那么对于一切 $b\in B$，都有 $a\leqslant b$，即 a 是 B 的一个下界，因而 $a\leqslant d$. 另外，如果 x 是 A 的一个上界，则 $x\in B$. 由 d 的选取，$d\leqslant x$. 所以 $d=\sup A$. 因而 L 是完全格.

四、子格

定义 3 格 $\langle L,\leqslant\rangle$ 的非空子集 M 关于 L 中的 $\vee$ 和 $\wedge$ 两种运算封闭，则称为 L 的子格.

由定理 2，子格也是格，而且与原格的运算一致.

格的全序子集显然是子格. 特别，格的任一单元素自成子格.

例 6 任意群 G 的所有正规子群，按包含关系作成 G 的子群格的子格.

证明：设 G 的所有正规子群作成集合 $\sum$. 任取 N_1，$N_2\in\sum$，则在子群格中，$N_1\vee N_2=\langle N_1\cup N_2\rangle=N_1N_2=N_2N_1$（参见复习题三第 29 题），仍是 G 的正规子群，即 $\sum$ 关于 $\vee$ 封闭. $N_1\wedge N_2=N_1\cap N_2$ 也是 G 的正规子群，即 $\sum$ 关于 $\wedge$ 也封闭. 即 $\sum$ 作成子群格的子格.

例 7 图 7—6 对应的半序集显然作成格，设为 $\langle L,\leqslant\rangle$.

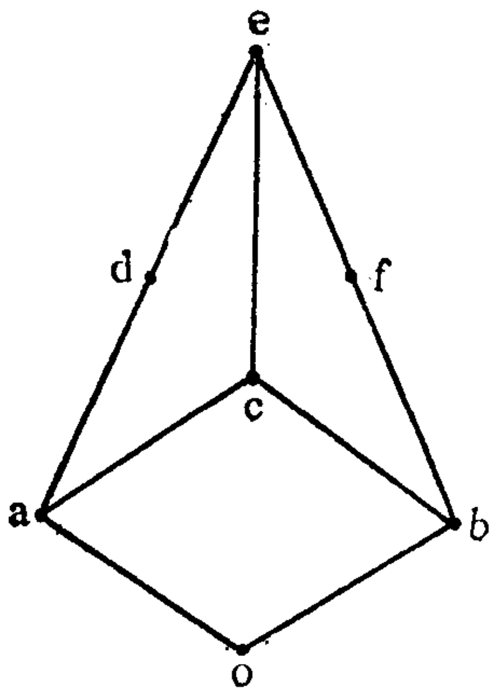


图 7—6

令 $L_1=\{o, a, b, c\}$，$L_2=\{o, a, b, e\}$。L_1 是 L 的子格。L_2 虽也作成格，但不是 L 的子格，因为在 L 中 $a\vee b=c\notin L_2$。这说明格的子集尽管作成格，却不见得是子格。

例 8 设 $\langle L,\leqslant\rangle$ 是格，$a\in L$。取 $L_a=\{x\in L|x\leqslant a\}$，$M_a=\{x\in L|a\leqslant x\}$，则 L_a 和 M_a 都是 L 的子格。

证明：任取 $x, y\in L_a$，则 $x\leqslant a$，$y\leqslant a$，由上确界定义，$x\vee y\leqslant a$，又 $x\wedge y\leqslant x\leqslant a$，故 $x\vee y$，$x\wedge y\in L_a$，L_a 是子格。同法可证 M_a 也是子格。

五、格的同态与同构

定义 4 设 $\langle A,\leqslant\rangle$ 和 $\langle B,\leqslant\rangle$ 是半序集，如果 φ 是 A 到 B 的映射，具有保序性质，即当 $a\leqslant b$ 时，$\varphi(a)\leqslant\varphi(b)$，则称 φ 是保序映射。

例 9 $\boldsymbol{C}$ 到 $\boldsymbol{R}$ 的映射 φ 规定为 $\varphi(a+bi)=a$，则 φ 是 $\langle\boldsymbol{C},\leqslant\rangle$ 到 $\langle\boldsymbol{R},\leqslant\rangle$ 的保序映射。

例 10 $\boldsymbol{R}$ 到 $\boldsymbol{R}$ 的映射 φ 规定为 $\varphi(x)=2x+5$，则 φ 是 $\langle\boldsymbol{R},\leqslant\rangle$ 到自身的保序映射，因为由 $x_1\leqslant x_2$，可以推出 $2x_1+5\leqslant 2x_2+5$。

例 11 设 $\langle A,\leqslant\rangle$ 是半序集，对于 $a\in A$，设 $\varphi(a)=\{x|x\in A, x\leqslant a\}$，则 φ 是 $\langle A,\leqslant\rangle$ 到 $\langle F(A),\subseteq\rangle$ 的保序映射。事

实上，如果 $a\leqslant b$，则显然 $\varphi(a)\subseteq\varphi(b)$。

定义 5 设 $\langle L_1,\leqslant\rangle$ 和 $\langle L_2,\leqslant\rangle$ 是格，如果存在 L_1 到 L_2 的映射 φ，使对 a，$b\in L_1$、有

$$\varphi(a\vee b)=\varphi(a)\vee\varphi(b),\quad \varphi(a\wedge b)=\varphi(a)\wedge\varphi(b),$$

则称 φ 是格 L_1 到格 L_2 的同态。如果 φ 是同态且是满射，则称为满同态，这时称格 L_1 和 L_2 同态。如果 φ 是同态又是一一映射，则称 φ 是格 L_1 到格 L_2 的同构，这时称格 L_1 和 L_2 同构，记为 $L_1\cong L_2$。

定理 5 如果 φ 是格 L_1 到 L_2 的同态，则 φ 是保序映射。

证明：设 a，$b\in L_1$，$a\leqslant b$，则 $a\wedge b=a$，$\varphi(a)=\varphi(a\wedge b)=\varphi(a)\wedge\varphi(b)\leqslant\varphi(b)$。$\varphi$ 是保序映射。

证毕

注意：定理 5 的逆不成立。如例 11 中，取 $A=C$，关于半序 $\leqslant$ 作成格，设 $a=0$，$b=1-i$，则 $a\vee b=1$。

$\varphi(a)=\{x+yi\,|\,x\leqslant 0,\ y\leqslant 0\}$，

$\varphi(b)=\{x+yi\,|\,x\leqslant 1,\ y\leqslant -1\}$，

$\varphi(a\vee b)=\{x+yi\,|\,x\leqslant 1,\ y\leqslant 0\}$。

而 $\varphi(a)\vee\varphi(b)=\varphi(a)\cup\varphi(b)\neq\varphi(a\vee b)$，因为 $1\in\varphi(a\vee b)$，$1\overline{\in}\varphi(a)\vee\varphi(b)$。（如图 7—7）

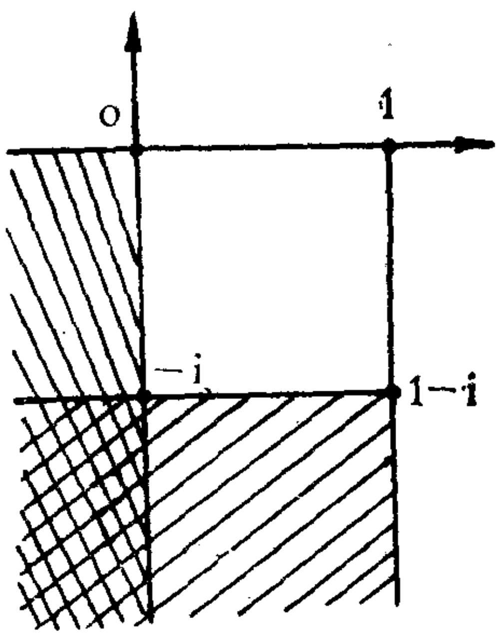


图 7—7

这说明格的同态要比保序映射条件更高。下面利用保序映射给出判断格同构的准则：

定理 6 格 L_1 到 L_2 的一一映射 φ 是同构的充要条件为

φ 和 φ^{-1} 都是保序映射.

证明：设 φ 是同构，显然 φ^{-1} 也是同构，由定理 5，φ 和 φ^{-1} 是保序的. 反之，假定 φ 是保序的一一映射，任取 $a, b \in L_1$，则

$$\varphi(a) \leqslant \varphi(a \vee b),\quad \varphi(b) \leqslant \varphi(a \vee b),$$

从而 $\varphi(a) \vee \varphi(b) \leqslant \varphi(a \vee b)$. 由于 φ 是一一映射，在 L_1 中必有 m，使 $\varphi(m) = \varphi(a) \vee \varphi(b)$，则 $\varphi(m) \leqslant \varphi(a \vee b)$. 又 $\varphi(a) \leqslant \varphi(m)$，$\varphi(b) \leqslant \varphi(m)$，$\varphi^{-1}$ 保序，故 $a \leqslant m$，$b \leqslant m$，$a \vee b \leqslant m$. $\varphi(a \vee b) \leqslant \varphi(m) = \varphi(a) \vee \varphi(b)$，所以 $\varphi(a) \vee \varphi(b) = \varphi(a \vee b)$.

同理，$\varphi(a) \wedge \varphi(b) = \varphi(a \wedge b)$. φ 为格同构.

证毕

习 题 7·2

1. 求证在格中：

(1) $a \leqslant b$ 且 $a \leqslant c$ 当且仅当 $a \leqslant b \wedge c$；

(2) $a \leqslant c$ 且 $b \leqslant c$ 当且仅当 $a \wedge b \leqslant c$；

(3) 若 $a \leqslant b$ 且 $c \leqslant d$，则 $a \vee c \leqslant b \vee d$，$a \wedge c \leqslant b \wedge d$；

(4) 若 $a \leqslant b \leqslant c$，$d \wedge c = a$，则 $d \wedge b = a$；

(5) 若 $a \leqslant b \leqslant c$，$d \vee a = c$，则 $d \vee b = c$；

(6) $a \wedge (b \wedge c) \leqslant (a \wedge b) \wedge (a \vee c)$；

*(7) $(a \wedge b) \vee (a \wedge c) \leqslant a \wedge (b \vee c)$；

*(8) $[(a \wedge b) \vee (a \wedge c)] \wedge [(a \wedge b) \vee (b \wedge c)] = a \wedge b$.

2. 求证：半序集是完全格的充要条件是存在最小元，且任一子集有上确界.

3. 区间(0,1)的有理数集按大小是否作成完全格？

4. 正整数集 P 关于整除关系是否作成完全格?

5. 求证定理 1(L_4)中的第二式.

6. 设格 L_1 与 L_2 同态，如果 L_1 有单位元，则 L_2 也有；如果 L_1 有零元，则 L_2 也有. 试证明之.

7. 写出 B_4 子群格的所有四元子格.

8. 证明定理 1 中(L_1)可由(L_2)、(L_3)、(L_4)推出.

9. 求证：两子格的交仍是子格.

10. 设格中 $a \leqslant b$，求证：集合

$$\{x \mid a \leqslant x \leqslant b\}$$

作成子格.

§7·3 分配格与模格

本节介绍两种重要的格：分配格与模格，前者是后者的特殊情形.

一、分配格

在集合的子集格$\langle F(S), \subseteq\rangle$中，成立着两种分配律：对于$S$的任意子集$A, B, C$，有

$$(D_1) \qquad A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$(D_2) \qquad A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

(见§1·1 定理 1)

$\cap$和$\cup$在子集格中即$\wedge$和$\vee$运算，在一般的格中这两种运算之间的联系不一定这样紧密，如三次对称群 S_3 的子群格中，设$H_1 = \{(1), (1\ 2)\}$，$H_2 = \{(1), (1\ 3)\}$，$H_3 = \{(1), (2\ 3)\}$，但

$$H_1 \wedge (H_2 \vee H_3) = H_1 \wedge S_3 = H_1,$$

$$(H_1 \wedge H_2) \vee (H_1 \wedge H_3) = \{(1)\} \vee \{(1)\} = \{(1)\}.$$

所以，(D_1)不成立。

定义 1 (D_1)和 (D_2) 成立的格称为分配格。

例 1 任意集合的子集格是分配格。

例 2 全序集是分配格。事实上，任取元素 a, b, c。若 $b \leqslant a$ 且 $c \leqslant a$，则

$a \wedge (b \vee c) = b \vee c$，$(a \wedge b) \vee (a \wedge c) = b \vee c$；若 $a \leqslant b$ 或 $a \leqslant c$，则

$$a \wedge (b \vee c) = a, \quad (a \wedge b) \vee (a \wedge c) = a.$$

所以 (D_1) 成立，同法可证 (D_2) 也成立。

例 3 设格 L 的覆盖图如图 7—2，求证 L 是分配格。

证明： 当 a, b, c 中有 o 或 e 时，或当 a, b, c 中有相等元素时，$(D_1)(D_2)$显然成立。其余情况共有 $3! = 6$ 种，而由$\vee$的可换性，只须证明三种：

$$x \wedge (y \vee z) = x = (x \wedge y) \vee (x \wedge z).$$

$$y \wedge (x \vee z) = x = (y \wedge x) \vee (y \wedge z).$$

$$z \wedge (x \vee y) = x = (z \wedge x) \vee (z \wedge y).$$

所以，(D_1)成立，同法可证(D_2)。L 是分配格。

实际上，(D_1)和 (D_2) 有一成立即是分配格。

定理 1 在格中，(D_1)与(D_2) 等价。

证明： 如果 (D_1) 成立，则

$$\begin{aligned} a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) \\ &= a \vee [(a \wedge c) \vee (b \wedge c)] \\ &= a \vee [(a \vee b) \wedge c] \\ &= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] \end{aligned}$$

$$= (a \vee b) \wedge (a \vee c).$$

即(D_2)成立。反之，如果(D_2)成立，则

$$\begin{aligned} a \wedge (b \vee c) &= [a \wedge (a \vee c)] \wedge (b \vee c) \\ &= a \wedge [(a \vee c) \wedge (b \vee c)] \\ &= a \wedge [(a \wedge b) \vee c] \\ &= [(a \wedge b) \vee a] \wedge [(a \wedge b) \vee c] \\ &= (a \wedge b) \vee (a \wedge c). \end{aligned}$$

即(D_1)成立。

证毕

二、模格

分配格要求格的两种运算有较强的联系，许多重要的格(如正规子群格、理想格等)不是分配格。下面提出一类条件稍弱的格，使其概括一些常见的格。

定义 2 格 L 中，如当 $b \leqslant a$ 时 (D_1) 成立，则称为模格或狄特金 (Dedekind) 格[注]。

如果 $b \leqslant a$，$a \wedge b = b$，(D_1)化为

$$(M) \qquad a \wedge (b \vee c) = b \vee (a \wedge c).$$

另外，由 $b \leqslant a$，$b \leqslant b \vee c$，$a \wedge c \leqslant a, a \wedge c \leqslant c \leqslant b \vee c$，所以 (M) 中总有右端$\leqslant$左端。这样，模格的要求集中起来，就是：当 $b \leqslant a$ 时，

$$(M_1) \qquad a \wedge (b \vee c) \leqslant b \vee (a \wedge c).$$

下面举出模格的一个判别方法。

定理 2 格 L 是模格的充要条件是：如果 $b \leqslant a$，$a \vee c$

注 R. Dedekind(1831—1916)，德国数学家。

$=b\vee c$，$a\wedge c=b\wedge c$，则 $a=b$。

证明：若 L 是模格，假定 $b\leqslant a$，$a\vee c=b\vee c$，$a\wedge c=b\wedge c$，则

$$a=a\wedge(a\vee c)=a\wedge(b\vee c)=b\vee(a\wedge c)$$
$$=b\vee(b\wedge c)=b.$$

反之，设 L 是适合定理条件的格。若 $b\leqslant a$，$c\in L$，由 (M_1) 前面分析的结果，

$$b\vee(a\wedge c)\leqslant a\wedge(b\vee c).$$

于是

$$a\wedge c=a\wedge(c\wedge c)=(a\wedge c)\wedge c$$
$$\leqslant[b\vee(a\wedge c)]\wedge c\leqslant[a\wedge(b\vee c)]\wedge c$$
$$=a\wedge c,$$
$$[a\wedge(b\vee c)]\wedge c=[b\vee(a\wedge c)]\wedge c, \qquad (1)$$

同样可以证明

$$[a\wedge(b\vee c)]\vee c=b\vee c,$$
$$[b\vee(a\wedge c)]\vee c=b\vee c.$$

即 $[a\wedge(b\vee c)]\vee c=[b\vee(a\wedge c)]\vee c$。与 (1) 式相连可以推出 $a\wedge(b\vee c)=b\vee(a\wedge c)$。所以 L 是模格。

证毕

定理 3 任意群的正规子群格是模格。

证明：设 Σ 是 G 的正规子群格，$A,B,C\in\Sigma$，假定 $B\leqslant A$（即 $B\subseteq A$）而 $A\wedge(B\vee C)=A\cap BC$，$B\vee(A\wedge C)=B(A\wedge C)$。

$A\cap BC$ 的元素形如 $a=bc\in A$，$b\in B$，$c\in C$。因而 $c=b^{-1}a\in A$（因为 $B\subseteq A$）。所以 $c\in A\cap C$，$a\in B(A\cap C)$，$A\cap BC\subseteq B(A\cap C)$。因而 $A\wedge(B\vee C)\leqslant B\vee(A\wedge C)$，$(M_1)$ 成立。

证毕

由此可知可换群的子群格是模格．同样方法可以证明环的理想格是模格（留作习题）．

*三、模格中的覆盖链

设 a，b 是模格 L 的元素，$a\leqslant b$．集合 $\{x\in L\mid a\leqslant x\leqslant b\}$ 显然是 L 的子格，称为商格，记为 b/a．以下定理类似于群的第二同构定理(§ 3·10)：

定理 4 设 a，b 为模格 L 中的元素，则

$$b/a\wedge b\cong a\vee b/a.$$

证明：任取 $x\in b/a\wedge b$，即 $a\wedge b\leqslant x\leqslant b$．规定 $f(x)=x\vee a$。显然 $a\leqslant f(x)\leqslant a\vee b$，$f(x)\in a\vee b/a$．

f 是单射．事实上，若 x，$y\in b/a\wedge b$，$x\neq y$，使 $f(x)=f(y)$，不妨设 $x\vee y\neq x$，因而 $x<x\vee y$，$a\wedge b\leqslant x\vee y\leqslant b$．故

$$(x\vee y)\vee a=(x\vee a)\vee(y\vee a)=f(x)\vee f(y)$$
$$=f(x)=x\vee a.$$
$$(x\vee y)\wedge a=a\wedge b=x\wedge a.$$

根据定理 2，推得 $x\vee y=x$，矛盾．

f 是满射．事实上，任取 $y\in a\vee b/a$，则由模格性质，$y=(a\vee b)\wedge y=a\vee(b\wedge y)$．$f(b\wedge y)=a\vee(b\wedge y)=y$．

f 是保序的．事实上，若 $x\leqslant y$，$x,y\in b/a\wedge b$，则 $x\vee a\leqslant y\vee a$，即 $f(x)\leqslant f(y)$．反之，若 $f(x)\leqslant f(y)$，则 $x\vee a\leqslant y\vee a$，

$$f(x\vee y)=(x\vee y)\vee a=(x\vee a)\vee(y\vee a)=y\vee a=f(y).$$

由于 f 是一一映射，故 $x\vee y=y$，$x\leqslant y$．由上节定理 6，$b/a\wedge b$ 与 $a\vee b/a$ 格同构．

证毕

定理 5 在模格中，如果从零元 0 到 x 存在有限的覆盖链，则任一这种覆盖链有相同的长度，其长度由 x 唯一决定。

证明： 设有 0 到 x 的两个覆盖链：

$$0=x_0<x_1<\cdots<x_{n-1}<x_n=x; \tag{1}$$

$$0=y_0<y_1<\cdots<y_{m-1}<y_m=x. \tag{2}$$

对 n 实行归纳法。若 $n=1$，x 覆盖 0，显然成立。设对于小于 n 的情况结论正确，下面讨论 n 的情况。若 $x_{n-1}=y_{m-1}$，由归纳假定，从 0 到 x_{n-1} 长度为 $n-1$，因而 $m-1=n-1$，$m=n$。如果 $x_{n-1}\neq y_{m-1}$，由于 x 覆盖 x_{n-1} 和 y_{m-1}，故 $x=x_{n-1}\vee y_{m-1}$。由上一定理，

$$x/x_{n-1}\cong y_{m-1}/x_{n-1}\wedge y_{m-1},\quad x/y_{m-1}\cong x_{n-1}/x_{n-1}\wedge y_{m-1}.$$

由于 x 覆盖 x_{n-1} 和 y_{m-1}，故 x_{n-1} 和 y_{m-1} 覆盖 $x_{n-1}\wedge y_{m-1}$。(1) 中从 0 到 x_{n-1} 的覆盖链长为 $n-1$，由归纳假定，从 0 到 x_{n-1} 的所有覆盖链长为 $n-1$。所以从 0 到 $x_{n-1}\wedge y_{m-1}$ 的覆盖链长为 $n-2$。从 0 到 $x_{n-1}\wedge y_{m-1}$ 的任一覆盖链都可延伸到 y_{m-1}，因而这一从 0 到 y_{m-1} 的覆盖链长为 $n-2+1=n-1$，利用归纳假定，可知任意从 0 到 y_{m-1} 的覆盖链长为 $n-1$，(2) 中的这一覆盖链长 $m-1$，故 $m-1=n-1$，$m=n$。

证毕

由于覆盖链长的唯一性，可以规定 $d(x)$ 为 0 到 x 覆盖链的长度，称为 x 的维数。

推论 1 （约当一狄特金）在模格中，两个元素之间的所有有限覆盖链有相同长度。

证明： 如果 $b<a$，在商格 a/b 中，b 为零元。由定理 5，可得结论。

证毕

如果两元素的维数存在，那末显然从 a 到 b 的覆盖链 $(a<b)$ 长等于 $d(b)-d(a)$。特别，由于 $x\vee y/x\cong y/x\wedge y$，故从 x 到 $x\vee y$ 与从 $x\wedge y$ 到 y 的覆盖链如果存在则必同长，因而在元素有限的模格中

$$d(x\vee y)-d(x)=d(y)-d(x\wedge y),$$

或

$$d(x)+d(y)=d(x\vee y)+d(x\wedge y)。\tag{3}$$

上式称为维数公式。可以证明，**维数公式成立的格也一定是模格。**

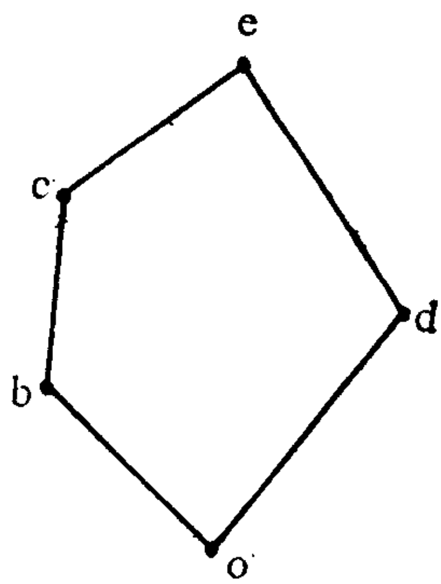


图 7—8

例 4 设有格 $L=\{o, b, c, d, e\}$，其覆盖图如图 7—8。$o<b<c<e$ 和 $o<d<e$ 都是从 o 到 e 的覆盖链，但长度不同，由定理 5，知 L 不是模格。

反之，可以证明，任何非模格总有一个子格的覆盖图是上述五边形。

习　题　7·3

1. 求证：$\langle \mathbf{C}, \leqslant\rangle$ 是分配格。

2. 设 L 是分配格，a 是 L 的固定元素，规定 $\varphi(x)=x\wedge a$，$\psi(x)=x\vee a$ $(x\in L)$，求证：φ 和 ψ 都是格 L 的自同态，$\varphi[L]$ 和 $\psi[L]$ 是 L 的子格。

3. 作出 A_4 子群格的覆盖图。这一格是否模格？

4. 克莱茵四元群 B_4 的子群格是否分配格？

*5. 求证：环的理想格（§7·2例5）是模格.

6. 求证：分配格或模格的同态象及子格也是分配格或模格.

本 章 提 要

一、半序集：具有满足反身性、反对称性、传递性的关系的集合.

二、格：半序集中任意两个元素都有上、下确界时，叫做格. 任意子集都有上、下确界的格，称为完全格.

三、分配格：$\vee$和$\wedge$之间适合分配律的格.

四、模格：适合下式的格：

当 $b\leqslant a$ 时，$a\wedge(b\vee c)\leqslant b\vee(a\wedge c)$.

分配格是模格，反之不然.

任意集合的子集格是分配格，任意群的正规子群格以及任意环的理想格是模格.

复 习 题 七

1. 作出正方形对称群 D_4 的子群覆盖图.

*2. 设Σ是集合A的所有关系组成的集合，在Σ中规定$\leqslant$如下：$R_1\leqslant R_2\Longleftrightarrow$若 aR_1b，则 aR_2b. 求证：$\langle\Sigma,\leqslant\rangle$是半序集，且同构于 $A\times A$ 的子集包含半序集. Σ的单位元和零元是什么?

3. 设$\langle L,\leqslant\rangle$是半序集，$S$ 是集合，F 是S到L的映射的全体组成的集合. 在F中规定 $f\leqslant g$ 当且仅当对于 $x\in S$,

有 $f(x)\leqslant g(x)$. 求证：$\langle F,\leqslant\rangle$ 是半序集；如果 L 是格，F 也是格。

4. 设 o 和 e 是格 L 的零元和单位元，求证：对于 $a, b\in L$，有

(1) $o\vee a=a$, $o\wedge a=o$;

(2) $e\vee a=e$, $e\wedge a=a$;

(3) 若 $a\vee b=o$, 则 $a=b=o$;

(4) 若 $a\wedge b=e$, 则 $a=b=e$.

5. 在任意格 L 中，求证：L 关于 $\vee$ 和 $\wedge$ 各作成可换半群。若 L 有单位元和零元，那么 L 的这两个元素在两个半群中起什么作用？

*6. 求证：格 L 是模格的充要条件是对于 $a,b,c\in L$，有恒等式

$$a\wedge[(a\wedge b)\vee c)]=(a\wedge b)\vee(a\wedge c).$$

*7. 在分配格中，求证：由 $a\wedge c=b\wedge c, a\vee c=b\vee c$，可推出 $a=b$.

8. 求证：2^n 阶循环群的子群格是分配格。

9. 求证：在任意格中，有

$$[(a\vee b)\wedge(a\vee c)]\vee[(a\vee b)\wedge(b\vee c)]=a\vee b.$$

10. 求证：在格中，如果 c 覆盖 a 和 b，且 $a\neq b$，则 $c=a\vee b$；如果 a 和 b 都覆盖 c，且 $a\neq b$，则 $c=a\wedge b$.

11. 求证：在格中，任意极大元都是单位元，因而极大元不超过一个，同样的结论对极小元和零元也成立。对一般的半序集这个结论也成立吗？举一反例。

习题答案与提示

习题1·1

1．(1) $0\in M_1,M_2,M_3,M_5$；$1\in M_1,M_2,M_3,M_4,M_5$；$\frac{3}{5}\in M_3,M_4,M_6$；$\sqrt{2}\in M_3,M_4,M_6$；$-2\in M_2,M_3,M_6$；$\pi\in M_3,M_4,M_6$；$-\frac{1}{7}\in M_3,M_6$．(2) $M_5\subset M_1\subset M_2\subset M_3$，$M_4\subset M_3$，$M_6\subset M_3$．(3) $M_1\cap M_2=M_1$，$M_3\cup M_4=M_3$，$M_5\cup M_6=M_3$，$M_4\cap M_5=\{1\}$，$M_5\cap M_6=\phi$．

2．$|M|=3$．其根为0,1(重根)，-1(重根)．

3．(3) $A\subseteq A\cup B=B$；(4) $A=A\cap B\subseteq B$．

5．若$A=B$，则$A\cup B=A\cup A=A=A\cap A=A\cap B$；反之，若$A\cup B\subseteq A\cap B$，任取$x\in A$，则$x\in A\cup B\subseteq A\cap B\subseteq B$，即$A\subseteq B$，同理$B\subseteq A$．

6．设$x\in$左集．如果$x\in A$，则$x\in A\cup B$，$x\in A\cup C$，$x\in$右集；如果$x\in B\cap C$，则$x\in B,x\in C$，显然也属于右集．设$x\in$右集，如果$x\in A$，则$x\in$左集．否则$x\in B$且$x\in C$，即$x\in B\cap C\subseteq$左集．

7．(1) 全平面；(2) A_1．

8．(1) P；(2) 原点；(3) A_l，$l=[i,j]$；(4) i的倍数与j的倍数组成的自然数集合．

9．设这一带形区域为L．显然各$A_x\subseteq L$，故$\bigcup_{x\in R}A_x\subseteq L$．

反之，任取点$(x,y)\in L$，则以点$(x,0)$为心的圆A_x包含(x,y)。

10. 显然$(A\setminus B)\cup B\subseteq A\cup B$；反之，任取$x\in A\cup B$，若$x\in B$，则$x\in(A\setminus B)\cup B$，若$x\bar{\in}B$，则$x\in A\setminus B\subseteq(A\setminus B)\cup B$。故第一式成立。第二式显然。第三式的证明：设$x\in A$。若$x\in B$，则$x\in A\cap B$；若$x\bar{\in}B$，则$x\in A\setminus B$。左集$\subseteq$右集。反之显然。

11. 设$x\in A$，$x\bar{\in}B\cup C$，则$x\in A\setminus B$且$x\in A\setminus C$，即$x\in(A\setminus B)\cap(A\setminus C)$。反之显然。

12. $C_n^0+C_n^1+\cdots+C_n^n=2^n$。用归纳法证明。

习题1·2

1. (1) 一一变换；(2) 变换；(3) 不是变换 ($a=1$时无象)；(4) 不是变换($a\leqslant-1$时无象)；(5) 不是变换($a<-1$时无象)；(6) 一一变换；(7) 单射变换；(8) 满射变换。

2. (2) 0,1；(6) 0,1,−1；(7) 所有负数；(8) 所有负数。

3. $\sigma\tau(1)=1$，$\sigma\tau(2)=2$，$\sigma\tau(3)=3$，$\sigma\tau(4)=1$；$\tau\sigma(1)=2$，$\tau\sigma(2)=2$，$\tau\sigma(3)=3$，$\tau\sigma(4)=4$。

4. 由定理2，$\sigma^{-1}\sigma=\sigma\sigma^{-1}=\varepsilon_A$。又由定理3，$\sigma$是$\sigma^{-1}$的逆变换。

5. $(\sigma\tau)(\tau^{-1}\sigma^{-1})=(\tau^{-1}\sigma^{-1})(\sigma\tau)=\varepsilon_A$。

6. $|A\setminus B|=|A|-|B|=0$，$A\setminus B=\phi$，$A=B$。

7. 令 $f(n)=\begin{cases}2n, & \text{当 } n\geqslant 0 \text{ 时；}\\ -2n-1, & \text{当 } n<0 \text{ 时。}\end{cases}$ 则f是$\boldsymbol{Z}$到$\boldsymbol{N}$的一一映射，故$\boldsymbol{Z}\sim\boldsymbol{N}$。

8. 设φ是A到B的映射。满射时，$|B|=|\varphi[A]|\leqslant|A|$；单射时，$|A|=|\varphi[A]|\leqslant|B|$。

9. 设φ是满射，不是单射，必有$|A|>|\varphi[A]|=|B|$；设φ是单射，不是满射，则$|A|=|\varphi[A]|<|B|$。都有矛盾。对无限集的反例见第1题(7)、(8)。

10. (1)恒等变换ε_A是一一映射；(2)设σ是A到B的一一映射，则σ^{-1}是B到A的一一映射；(3)设σ,τ分别是A到B，B到C的一一映射，则$\tau\sigma$是A到C的一一映射。

习题1·3

1. 只有(4)、(5)、(10)是等价关系。

2. (4) 每类由实部相同的全体复数组成；(5) 每类由z与$-z$组成；(6) 几何上，每类由平行于z_0的一条直线组成。

3. 等价类由B中一个元素的全体原象组成。

4. 15种。

5. 几何上，是以O为心的圆。

6. (1) $A=EAE^{-1}$；若$B=TAT^{-1}$，则$A=T^{-1}B(T^{-1})^{-1}$；若$C=SBS^{-1}$，$B=TAT^{-1}$，则$C=STAT^{-1}S^{-1}=(ST)A(ST)^{-1}$。(2) $A=EAE'$；若$B=PAP'$，则$A=P^{-1}B(P^{-1})'$；若$C=SBS'$，$B=TAT'$，则$C=(ST)A(ST)'$。

7. 对于任意的$a,b\in A$，适合$a\rho c$，$c\sigma b$的c是否存在是完全确定的，故τ是关系。当ρ和σ是等价关系时，τ不一定是等价关系。

习题1·4

1. 设$A=\{a_1,\cdots,a_m\}$，$B=\{b_1,\cdots,b_n\}$，则$A\times B=\{a_1b_1,$

$\cdots,a_1b_n,\cdots,a_mb_1,\cdots,a_mb_n\}$.

2. 当n为偶数时，取$|A_1|=|A_2|=\frac{n}{2}$；当n为奇数时，取$|A_1|=\frac{n+1}{2}$.

3. (1) $S_R=\{(b+1,b)|b=0,1,2,\cdots\}$；(2) $S_R=\{(2b,b)|b=0,1,2,\cdots\}$；(3) $S_R=\{(a,b)|(a,b)=1,\ b=0,1,2,\cdots\}$；(4) $S_R=\{(5k+b,b)|b=0,1,2,\cdots,5k+b\geqslant 0,k\in \mathbf{Z}\}$；(5) $S_R=\{(5k-b,b),b=0,1,2,\cdots,5k-b\geqslant 0,\ k\in \mathbf{Z}\}$.

4. 等价类形如$\{(x,b)|x\in A\}$，$b\in B$. 让它对应$b\in B$，则作成$(A\times B)/E$到B的一一映射.

5. $\bar{A}$的元素形如$[a]=\{x|\sigma(x)=\sigma(a)\}$，令$[a]\to\sigma(a)\in B$，可以证明这是$\bar{A}$到$B$的一一映射.

6. 等价关系显然. Z_n/E的元素是等价类$[[a]]=\{[x]\ |m|x-a\}$，$a\in \mathbf{Z}_n$. 令$[[a]]\to[r]\in \mathbf{Z}_m$，其中$r$是$a$用$m$除的余数. 这是一一映射.

7. 任取$re^{i\theta}\in \mathbf{C}^*$，令$re^{i\theta}\to(r,\theta)\in \mathbf{R}^+\times U$，这是$\mathbf{C}^*$到$\mathbf{R}^+\times U$的一一映射，$\mathbf{C}^*/E$的元素是等价类$P_r=\{re^{i\theta}|\theta\in U\}$ $(r>0)$. 令$P_r\to r$，则是$\mathbf{C}^*/E$到U的一一映射.

8. 任取$(a,x)\in A\times(B\cup C)$，则$a\in A$，$x\in B$或$C$，若$x\in B$，则$(a,x)\in A\times B$，否则$x\in C$，$(a,x)\in A\times C$. 反之，若$(a,x)\in(A\times B)\cup(A\times C)$，显然$(a,x)\in A\times(B\cup C)$. (1)得证. (2)式类似.

习题 1·5

1. (1)(2)(3)是代数运算.

2. 不是. 如$1\cdot 1=$? 没有规定.

3. 从代数运算定义可见.

4. 内积不是代数运算、因结果是数,不是 $\boldsymbol{R}_3$ 中的向量.

5. $2^4=16$.

6. (1) c,b,a; (2) a,a; (3) b,c.

复习题一

2. $\bigcup\limits_a S_a=\boldsymbol{R}$. $\bigcap\limits_a S_a=\phi$.

3. (1) 由于 $A\cup B=[A\backslash(A\cap B)]\cup[B\backslash(A\cap B)]\cup(A\cap B)$, 右端三个集合互不相交, 故 $|A\cup B|=|A\backslash(A\cap B)|+|B\backslash(A\cap B)|+|A\cap B|=|A|-|A\cap B|+|B|-|A\cap B|+|A\cap B|=|A|+|B|-|A\cap B|$. (2) 由(1), 左端 $=|A\cup B|+|C|-|(A\cup B)\cap C|=|A|+|B|-|A\cap B|+|C|-|(A\cap C)\cup(B\cap C)|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$.

4. 是映射. $\varphi[\boldsymbol{Z}]=\{0,1,2,3,4\}$. φ 不是单射. $\varphi^{-1}[1]=\{5k+1\,|\,k\in\boldsymbol{Z}\}$.

5. m^n.

6. φ 是单射, 不是满射, $\varphi[\boldsymbol{P}]=\boldsymbol{P}\backslash\{n,\ n+1,\ \cdots,\ 2n-1\}$.

7. 是单射也是满射, 因而是一一映射.

8. (1) 设 $gf=\varepsilon_A$, 若 $f(a_1)=f(a_2)$, 则 $a_1=\varepsilon_A(a_1)=(gf)(a_1)=g(f(a_1))=g(f(a_2))=(gf)(a_2)=\varepsilon_A(a_2)=a_2$. 即 f 是单射. 反之, 设 f 是单射, 在 A 中取定 a_0. 作 $g(b)=\begin{cases}a, & 如果\ f(a)=b;\\ a_0, & 如果\ b\ 无原象.\end{cases}$ 则 g 是 B 到 A 的映射. 对于 $a\in A$, 有 $(gf)(a)=g(f(a))=a$, 即 $gf=\varepsilon_A$. (2) 设 $fh=\varepsilon_B$, 任取

$b\in B$，则 $b=\varepsilon_B(b)=(fh)(b)=f(h(b))\in f[A]$，$f$ 是满射。反之，设 f 是满射，规定 $h(b)=a$，其中 a 是 b 在 f 下的任一确定的原象，h 是 B 到 A 的映射，且 $(fh)(b)=f(h(b))=f(a)=b$，即 $fh=\varepsilon_B$。

9. $(n-k)!$。

10. 任取 $A_1\subseteq A$，设 $B_1=A_1\cap B$，$C_1=A_1\cap C$，显然 $A_1\to(B_1,C_1)$ 是 $F(A)$ 到 $F(B)\times F(C)$ 的一一映射。

11. 任取 $c\in C$，由于 ψ 是满射，故有 $b\in B$，使 $\psi(b)=c$，同理有 $a\in A$，使 $\varphi(a)=b$，所以 $(\psi\varphi)(a)=c$，$\psi\varphi$ 是满射。对于单射或一一映射也成立。

12. (1) 设 $x\in\varphi[\bigcup_{i\in I}A_i]$，必有 $i\in I$，$a_i\in A_i$，$x=\varphi(a_i)\in\varphi[A_i]\subseteq\bigcup_{i\in I}\varphi[A_i]$。反之，设 $y\in\bigcup_{i\in I}\varphi[A_i]$，则必有 $i\in I$，使 $y\in\varphi[A_i]\subseteq\varphi[\bigcup_{i\in I}A_i]$。(2) 设 $x\in\varphi^{-1}[\bigcup_{i\in I}A_i]$，必有 $i\in I$，$\varphi(x)\in A_i$，$x\in\varphi^{-1}[A_i]\subseteq\bigcup_{i\in I}\varphi^{-1}[A_i]$。反之，任取 $y\in\bigcup_{i\in I}\varphi^{-1}[A_i]$，不妨设 $y\in\varphi^{-1}[A_i]$，则 $y\in\varphi^{-1}[\bigcup_{i\in I}A_i]$。(3) 设 $x\in\varphi^{-1}[\bigcap_{i\in I}A_i]$，则 $\varphi(x)\in\bigcap_{i\in I}A_i$，$x\in\varphi^{-1}[A_i]$ 对所有 $i\in I$ 成立，$x\in\bigcap_{i\in I}\varphi^{-1}[A_i]$。反之，设 $y\in\bigcap_{i\in I}\varphi^{-1}[A_i]$，则 $y\in\varphi^{-1}[A_i]$，$\varphi(y)\in A_i$ 对所有 $i\in I$ 成立。因而 $\varphi(y)\in\bigcap_{i\in I}A_i$，$y\in\varphi^{-1}[\bigcap_{i\in I}A_i]$。

13. 显然恒等变换 ε 适合 $\varepsilon\varepsilon=\varepsilon$。另一方面，若一一变换 φ 适合 $\varphi\varphi=\varphi$，两端同乘 φ^{-1} 则有 $\varphi(\varphi\varphi^{-1})=\varphi\varphi^{-1}=\varepsilon$，即 $\varphi\varepsilon$

$=\varepsilon$，$\varphi=\varepsilon$。

14．$\sigma(y)=\begin{cases}\dfrac{y}{2}，当 y 是偶数时；\\ \dfrac{y+1}{2}，当 y 是奇数时。\end{cases}$

15．由于关系与 $A\times A$ 的子集一一对应，而 $|A\times A|=n^2$，故 $A\times A$ 有 2^{n^2} 个子集（见习题1·1—12），A 中有 2^{n^2} 种不同的关系。A 中的一个代数运算相当于 $A\times A$ 到 A 的一个映射。由5题，共有 n^{n^2} 个映射，故 A 中共有 n^{n^2} 种不同的代数运算。

习题2·1

1．对于任意的 (a,b)，$(a_1,b_1)\in A\times B$，$(a,b)*(a_1,b_1)=(a\cdot a_1,b\circ b_1)$ 是 $A\times B$ 的唯一确定的元素。

2．由 · 和 ∘ 适合结合律，故 * 也适合结合律。

3．（1） 是。由于关于乘法封闭，且矩阵乘法适合结合律。（2） 不是。如 $(1\div i)\div(-i)=(-i)\div(-i)=1$，$1\div(i\div(-i))=1\div(-1)=-1$。（3） 是。因关于加法封闭，且适合结合律。（4） 不是。如 $(1+2i)^2=-3+4i$ 不属于这一集合。（5） 是。因关于乘法封闭，且适合结合律。

5．若 $\{a\}$ 是子半群，则由乘法封闭性 $a^2\in\{a\}$，即 $a^2=a$。反之，若 $a^2=a$，则 $\{a\}$ 关于乘法封闭。

6．依次为 d,c,c,d。如推断 $d\cdot a$，由 $d=c\cdot b$，知 $d\cdot a=(c\cdot b)\cdot a=c\cdot(b\cdot a)=c\cdot b=d$。

7．

	a	b
a	a	a
b	a	a

	a	b
a	a	b
b	a	b

8. 第一个半群的子半群有：$\{a,b\},\{a\}$；第二个半群的子半群有：$\{a,b\},\{a\},\{b\}$。

9. 由§1·2四，两变换之积仍为变换，且适合结合律。

10. T的子集也是S的子集，且显然T的子集的并与交仍是T的子集。

11.

(1)

∘	1	2	3	4	6	12
1	1	1	1	1	1	1
2	1	2	1	2	2	2
3	1	1	3	1	3	3
4	1	2	1	4	2	4
6	1	2	3	2	6	6
12	1	2	3	4	6	12

(2)

*	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

(3) 设$S_1=\{2,3\}$，$S_2=\{1,3\},S_3=\{1,2\}$，则$\bar{S}$的子集共有：$\bar{S}$，$S_1,S_2,S_3,\{1\},\{2\},\{3\},\phi$。

(3)

$\cap$	$\bar{S}$	S_1	S_2	S_3	$\{1\}$	$\{2\}$	$\{3\}$	ϕ
$\bar{S}$	$\bar{S}$	S_1	S_2	S_3	$\{1\}$	$\{2\}$	$\{3\}$	ϕ
S_1	S_1	S_1	$\{3\}$	$\{2\}$	ϕ	$\{2\}$	$\{3\}$	ϕ
S_2	S_2	$\{3\}$	S_2	$\{1\}$	$\{1\}$	ϕ	$\{3\}$	ϕ
S_3	S_3	$\{2\}$	$\{1\}$	S_3	$\{1\}$	$\{2\}$	ϕ	ϕ
$\{1\}$	$\{1\}$	ϕ	$\{1\}$	$\{1\}$	$\{1\}$	ϕ	ϕ	ϕ
$\{2\}$	$\{2\}$	$\{2\}$	ϕ	$\{2\}$	ϕ	$\{2\}$	ϕ	ϕ
$\{3\}$	$\{3\}$	$\{3\}$	$\{3\}$	ϕ	ϕ	ϕ	$\{3\}$	ϕ
ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ	ϕ

(4)

$\cup$	$\bar{S}$	S_1	S_2	S_3	$\{1\}$	$\{2\}$	$\{3\}$	ϕ
$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$	$\bar{S}$
S_1	$\bar{S}$	S_1	$\bar{S}$	$\bar{S}$	$\bar{S}$	S_1	S_1	S_1
S_2	$\bar{S}$	$\bar{S}$	S_2	$\bar{S}$	S_2	$\bar{S}$	S_2	S_2
S_3	$\bar{S}$	$\bar{S}$	$\bar{S}$	S_3	S_3	S_3	$\bar{S}$	S_3
$\{1\}$	$\bar{S}$	$\bar{S}$	S_2	S_3	$\{1\}$	S_3	S_2	$\{1\}$
$\{2\}$	$\bar{S}$	S_1	$\bar{S}$	S_3	S_3	$\{2\}$	S_1	$\{2\}$
$\{3\}$	$\bar{S}$	S_1	S_2	$\bar{S}$	S_2	S_1	$\{3\}$	$\{3\}$
ϕ	$\bar{S}$	S_1	S_2	S_3	$\{1\}$	$\{2\}$	$\{3\}$	ϕ

习题 2·2

1. 设 $bc=a$，则 $b(cx)=(bc)x=ax$。

2. 若 $T\subseteq W$，则 $(W\setminus T)\cup T=W$。反之，若在 $\langle F(S),\cup\rangle$ 中，$T|W$，则有 $V\in S$，使 $T\cup V=W$，即 $T\subseteq W$。另一

论断证法类似。

3。(1) 在$\langle \boldsymbol{P},\circ\rangle$中，$a|b \Longleftrightarrow$存在$c$使$(a,c)=b \Longleftrightarrow$通常意义下$b$整除$a$；(2) 设$e$是单位元，$e\circ 2e=(e,\ 2e)=e\neq 2e$,矛盾；(3) $n\circ 1=1\circ n=(1,n)=1$。在$\langle \boldsymbol{P},*\rangle$中,$a|b \Longleftrightarrow$在通常意义下$a$整除$b$；单位元是1；无零元。

4。设a，b是可逆元，$a=ae=(ab^{-1})b$, $a=ea=b(b^{-1}a)$。a的因子设为x，设$a=xb=cx$，则对于x的因子y，有$z,t\in A$，使$ty=x$，$yz=x$，$y(zba^{-1})=aa^{-1}=e$，$(a^{-1}ct)y=a^{-1}a=e$，即y是e的因子．由定理3，y可逆。

5。设0_1，0_2是两个左零元，对半群的任意元素x，有$(0_1 0_2)x=0_1(0_2 x)=0_1 0_2$，即$0_1 0_2$仍是半群的左零元。

6。设e_1，e_2是两个左单位元，对半群的任意元素x，有$(e_1 e_2)x=e_1(e_2 x)=e_1 x=x$。即$e_1 e_2$仍是半群左单位元。

8。设该集合为C．设$c_1,c_2\in C$，任取半群的元素x，则有y，z，使$xy=c_1$，$zx=c_2$，故$c_1c_2=x(yc_2)=(c_1z)x$,即x整除c_1c_2，$c_1c_2\in C$。

9。$\circ$是B中代数运算，且不论B中a，b，c是否属于A，总有$(a\circ b)\circ c=a\circ(b\circ c)$。对于任意$b\in B$，$b\circ u=u\circ b=b$，$u$是$B$的单位元。

10。类似上题。v是C的零元。

习题2·3

2。(2)，(4)。

3。(1)、(5)既约元；(4)、(8)可逆元；(2)、(3)、(6)、(7)可约元：$4=2\cdot 2$，$-20=-4\cdot 5$，$4=2\cdot 2$，$x^2-2=(x+\sqrt{2})\cdot(x-\sqrt{2})$。

4．A是$\langle \mathbf{R}^*,\cdot\rangle$的子半群，单位元是$1=\frac{3^0}{2^0}$；可逆元只有1；既约元有$3=\frac{3^1}{2^0}$和$\frac{1}{2}=\frac{3^0}{2^1}$；$\frac{3^2}{2^3}=\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{1}\cdot\frac{3}{1}$；$\langle A,\cdot\rangle$是唯一分解半群，因每一元素$\frac{3^m}{2^n}=\frac{1}{2}\cdots\frac{1}{2}\cdot\frac{3}{1}\cdots\frac{3}{1}$，且分解唯一。

5．$z=a+bi$可逆$\Longleftrightarrow$存在$c+di$，使$(a+bi)(c+di)=1$ $\Longleftrightarrow a^2+b^2=1\Longleftrightarrow z=\pm 1,\pm i$．若$1+2i=(a+bi)(c+di)$，则$(a^2+b^2)(c^2+d^2)=1^2+2^2=5$，或$a^2+b^2=1$，或$c^2+d^2=1$，因而$a+bi$或$c+di$是可逆元．

6．若$n>1$，则$n=1+\cdots+1$，且分解唯一．

7．设$3=(2+\sqrt{5}\,i)(a+b\sqrt{5}\,i)$，两端同乘$2-\sqrt{5}\,i$，得$6-3\sqrt{5}\,i=9a+9b\sqrt{5}\,i$，$9a=6$，不可能．

习题2·4

1．(1) 设$ac=b$，则$\sigma(a)\sigma(c)=\sigma(b)$；若$a$，$b$相伴，则$a|b,b|a,\sigma(a)|\sigma(b)$，$\sigma(b)|\sigma(a)$．(2)$f(n)=1$是$\langle \mathbf{Z}^*,\cdot\rangle$到$\langle\{1\},\cdot\rangle$的同态，既约元以及可约元的象都是可逆元1．$f(n)=[n]\in \mathbf{Z}_4(n\in\mathbf{Z})$是$\langle\mathbf{Z}^*,\cdot\rangle$到$\langle\mathbf{Z}_4,\cdot\rangle$的同态映射，但后者不是可消半群，如$[2][2]=[0]=[2][0]$．(见§2·1例7)

2．$\langle\mathbf{Z},+\rangle$有单位元0，奇数加半群无单位元．假如$\langle\mathbf{Z},+\rangle$与全体奇数作成的乘半群同态，则0的同态象应为单位元1．$\langle\mathbf{Z},+\rangle$每个元素可逆，但后者除1外均不可逆，如3无逆元．

3．由习题1·2—9，有限集的满射变换也是一一映射．

4. $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\to x$是$\langle M,\cdot\rangle$到$\langle \mathbf{R},+\rangle$的一一映射，且$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$ $\cdot\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & x+y\\ 0 & 1\end{pmatrix}\to x+y$，故上述映射也是同态，因而是同构。

5. $a\to\dfrac{1}{a}$是A到B的同构。

6. 注意：若$ab>1$，则至少有一因子>1。

7. (1)(3)是自同态。

8. 由例3，自同态形如(1)式。若$p\neq\pm1$，则1无原象，即$\varphi(a)=pa$不是一一映射。所以自同构只有恒等变换$(p=1)$和反号变换$(p=-1)$。

9. $a+b\sqrt{3}\to a+b\sqrt[3]{3}$是两加半群的同构。假如两乘群同构，单位元都是1，其可逆元应一一对应，前者的可逆元除±1外还有$1+\sqrt{2}$，$-1+\sqrt{2}$（因$(1+\sqrt{2})(-1+\sqrt{2})=1$）等，但后者的可逆元只有$\pm1$（设$(a+b\sqrt[3]{3})(c+d\cdot\sqrt[3]{3})=1$，则$ac+(ad+bc)\sqrt[3]{3}+bd\sqrt[3]{9}=1$，即$ac=1$，$bd=0$，$ad+bc=0$。得出$b=0$，$a=\pm1$，$c=\pm1$，$d=0$），出现矛盾。

10. 注意：可逆元与可逆元之积可逆，可逆元与不可逆元之积不可逆，不可逆元与不可逆元之积不可逆。

复习题二

1. (2)适合交换律，(3)适合结合律及交换律，(4)适合交换律。

2. $n^{\frac{n(n+1)}{2}}$。

3. 设 $A=(a_{ij}),b=(b_{ij})$. B是A的右因子等价于有X，使$XB=A$. 设$X=(x_{ij})$,则

$$\begin{cases} x_{k1}b_{11}+x_{k2}b_{21}+\cdots+x_{kn}b_{n1}=a_{k1}, \\ x_{k1}b_{12}+x_{k2}b_{22}+\cdots+x_{kn}b_{n2}=a_{k2}, \\ \cdots\cdots\cdots\cdots \\ x_{k1}b_{1n}+x_{k2}b_{2n}+\cdots+x_{kn}b_{nn}=a_{kn}, \quad k=1,2,\cdots,n, \end{cases}$$

成立. 这等价于$(a_{k1},a_{k2},\cdots,a_{kn})$可由$(b_{11},b_{12},\cdots,b_{1n})$, $(b_{21},b_{22},\cdots,b_{2n}),\cdots,(b_{n1},b_{n2},\cdots,b_{nn})$线性表示，等价于说$\begin{pmatrix} A \\ B \end{pmatrix}$与$B$等秩. 第二个断言类似可证.

4. 任取$a\in A$，则有$a_1,a_2\in A$，使$aa_1=e$，$a_1a_2=e$.因而$ea=eae=eaa_1a_2=eea_2=ea_2=aa_1a_2=ae=a$，$e$也是左单位元，即单位元. 而$a=ae=aa_1a_2=ea_2=a_2$，即$aa_1=a_1a_2=e$，$a_1$是$a$的逆元，$a$可逆.

5. (1) $(a*b)*c=\sqrt{a^2+b^2+c^2}=a*(b*c)$，故为半群，单位元是0；(2) $(a\circ b)\circ c=\max\{a,b,c\}=a\circ(b\circ c)$，故为半群，无单位元及零元；(3) $(a☆b)☆c=a+b+c+ab+bc+ac+abc=a☆(b☆c)$，故为半群，0为单位元，$-1$为零元；(4) $(a\circ b)\circ c=(a,b,c)=a\circ(b\circ c)$，故为半群，无单位元，零元为1；(5) $(a*b)*c=[a,b,c]=a*(b*c)$，故为半群，1为单位元，20为零元.

6. 当$p=q$时适合交换律，当$p=q=1$或$p=q=0$时适合结合律，当$p\neq0$且$q\neq0$时适合消去律.

7. $\mathbf{Q},\mathbf{Q},\mathbf{Q},\mathbf{Z},\mathbf{Q}^+$.

8. $\{a\},\{a,b\}$.

9. (1) 任取$k_1k\in K_1(K_2\cup K_3)$，则$k\in K_2\cup K_3$，不妨设k

$\in K_2$，则 $k_1k\in K_1K_2\subseteq K_1K_2\cup K_1K_3$。反之，设 $k_1k\in$ 右集，不妨设 $k_1k\in K_1K_2$，则 $k_1k\in$ 左集；(2)(3)同样可证。

10。除(4)外都是同态。

11。设 a，b 是幂等元，则 $(ab)^2=a^2b^2=ab$。

12。$a\to[a]\in\bar{A}$ 是 A 到 $\bar{A}$ 的映射，由于 $[a]\circ[b]=[ab]$ 故它是同态映射。

13。$\langle D^+,\cdot\rangle$ 是有单位元 1 的可换可消半群．可逆元只有 1，既约元是所有奇素数．任何正奇数可唯一地分解为奇素数之积，故为唯一分解半群．

14。任取 $x,y\in A$，$x\neq y$，所以 $xy\neq yx$。由于 $x^2x=xx^2$，故 $x^2=x$，x 是幂等元．又因

$$x(xyx)=x^2yx=xyx=xyx^2=(xyx)x,$$

所以 $x=xyx$。同法可证 $y=yxy$．反之，由于

$$(xy)(yx)=xy^2x=x,\quad (yx)(xy)=yx^2y=y,$$

可知当 $x\neq y$ 时，$xy\neq xy$。

习题 3·1

1。单位元是 2，a 的逆元是 $\frac{4}{a}$。

2。$(a*b)*c=a+b+c+ab+bc+ac+abc=a*(b*c)$。单位元是 0，$x=-\frac{1}{3}$。

3。$(a*b)*c=(b\cdot a)*c=c\cdot(b\cdot a)=(c\cdot b)\cdot a=(b*c)\cdot a=a*(b*c)$。单位元、逆元不变．

4。(2)、(3)、(4)、(5)是群．其中(4)的单位元是 1，x 的逆元是 $\frac{1}{x}$（当 $x>0$ 时）或 x（当 $x<0$ 时）。

习题 3·2

1. 若 $a^m=a^n$，则 $a^{m-n}=e$。

2. 设 a 的阶>2，则 $a^{-1}\neq a$ 且与 a 同阶，所以高于 2 阶的元素两两成对，共有偶数个，其他元素共有偶数个，去掉一阶元 e 后，共有奇数个二阶元。

3. 对于任意的 $x\in G$，有 $x^2=e$。设 $a,b\in G$，则 $(ab)^2=e$，或 $abab=e=a^2b^2$，$ba=ab$。

4. 设 $x^2=x$，则 $x^2x^{-1}=xx^{-1}=e$，$x=e$。

5. 若 G 可换，则 $(ab)^2=abab=a^2b^2$。反之，若 $(ab)^2=a^2b^2$，则 $abab=a^2b^2$，$ba=ab$。

6. 设 ab 的阶为 n，$(ab)\cdots(ab)=e$。因而 $ab\cdots ab=e$，$b(ab\cdots ab)=b$，$(bab\cdots a)b=b$，$bab\cdots a=e$。即 ba 的阶不大于 n；同理可证 ab 的阶不于 ba 的阶。所以 ab 与 ba 同阶。

7. 见第二题证明前半部。

8. 除$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$是一阶外，其他为二阶。

9. $a^n=e$，$(\bar{a})^n=\overline{a^n}=e$。

10. 设 a 的阶为 m，b 的阶为 n，$(ab)^{mn}=a^{mn}\cdot b^{mn}=e\cdot e=e$。

11. 设 abc 为 n 阶元，则 $a=ea=(abc)\cdots(abc)a=a(bca)^n$。即 $(bca)^n=e$，bca 的阶不大于 n。同理可证三个乘积阶数谁也不比谁高。

12. 任取 $a,b\in A$，由已知条件，存在 x_1,x_2,y_1,y_2 使 $a=x_1d$，$a=dy_1$，$d=x_2b$，$d=by_2$，因而 $a=(x_1x_2)b$，$a=b(y_2y_1)$，即 $a|b$，同理 $b|a$。所以 A 是群。

习题 3·3

1. $KH=\{kh|k\in K,\ h\in H\}\subseteq H$，但 $H=eH\subseteq KH$，故 $KH=H$，同理 $HK=H$。

2. 设 c_1，c_2 与 S 的任意元素 s 可换，$(c_1c_2)s=c_1(c_2s)=(c_1s)c_2=(sc_1)c_2=s(c_1c_2)$，即 c_1c_2 与 S 的元素可换，由 $c_1s=sc_1$ 两端左、右乘 c_1^{-1}，得 $sc_1^{-1}=c_1^{-1}s$ 即 c_1^{-1} 也与 S 的元素可换。e 显然也与 S 的元素可换。

3. 由定理 8，KH 是 G 的子群。$Ke=eK=K\subseteq KH$。

4. 任取 $\sigma(x)\in\bar{G}$，$x\in G$，则 x 可表为 $x=s_1^{k_1}\cdots s_n^{k_n}$。$\sigma(x)=\sigma(s_1)^{k_1}\cdots\sigma(s_n)^{k_n}\in\langle\sigma[S]\rangle$。

5. (1) $\{1,\ -1,\ i,\ -i\}$；(2) $\{2^{4k},\ 2^{4k+1}i,\ -2^{4k+2},\ -2^{4k+3}i\}(k=0,\pm1,\pm2,\cdots)$；(3) $\{(-1)^n2^k5^n\}(k,n=0,\pm1,\pm2,\cdots)$；(4) $\left\{1,-\dfrac{1}{2}+\dfrac{\sqrt{3}}{2}i,\ -\dfrac{1}{2}-\dfrac{\sqrt{3}}{2}i\right\}$。

6. 任取 $a\in G$，则 $\langle a\rangle$ 是 G 的子群。若 $\langle a\rangle$ 是有限群，则任取 $b\in G\backslash\langle a\rangle$，$\langle b\rangle$ 是 G 的又一子群，若 $\langle b\rangle$ 又是有限群，再取 $c\in G\backslash\langle a\rangle\backslash\langle b\rangle$，又得子群 $\langle c\rangle$，…。假若某子群，设为 $\langle a\rangle$ 是无限群，则 $\langle a^2\rangle\neq\langle a\rangle$，同理 $\langle a^3\rangle,\langle a^4\rangle$，…都是 G 的不同子群，所以无论何时 G 总有无限个互异的子群。

7. $G=\bigcup\limits_{a\in G}\langle a\rangle$，其中 $\langle a\rangle$ 是可换群。

8. 设 a，b 阶数不高于 2，则 $(ab)^2=a^2b^2=e,(a^{-1})^2=(a^2)^{-1}=e^{-1}=e$，说明积与逆阶数不高于 2。

9. 参考习题 3·2—10。

10. $g^{-1}h_1g\cdot g^{-1}h_2g=g^{-1}(h_1h_2)g\in g^{-1}Hg$，$(g^{-1}hg)^{-1}$

$=g^{-1}h^{-1}g\in g^{-1}Hg$，$e=g^{-1}eg\in g^{-1}Hg$。

11．$\{(1,d)\mid d\in R\}$。

12．任取 $h_1h_2\in$ 左集，则 $h_1h_2\in H_1H_2$，$h_1h_2\in H_1'$，因而 $h_2\in h_1^{-1}H_1'\subseteq H_1'$，同样 $h_1\in H_2'$，故 $h_1\in H_1\cap H_2'$，$h_2\in H_1'\cap H_2$，因而 $h_1h_2\in$ 右集．反之，$H_1\cap H_2'\subseteq H_1'\cap H_2'$，$H_1'\cap H_2\subseteq H_1'\cap H_2'$，$H_1\cap H_2'\subseteq H_1$，$H_1'\cap H_2\subseteq H_2$，因而

$$(H_1\cap H_2')(H_1'\cap H_2)\subseteq(H_1H_2)\cap H_1'\cap H_2'.$$

13．群的有限子群脉是有限可消子半群，故是子群。

习题 3·4

1．类似定理 1 的证明．

2．类似相应的证明．

3．$aH=\{ah\mid h\in H\}=\{ha\mid h\in H\}=Ha$。

4．设 $G=a_1H\cup\cdots\cup a_nH$，$H=b_1K\cup\cdots\cup b_mK$，则 $G=a_1b_1K\cup\cdots\cup a_1b_mK\cup\cdots\cup a_nb_1K\cup\cdots\cup a_nb_mK$。

5．任取 $ah\in aH$，$(ah)^{-1}=h^{-1}a^{-1}\in Ha^{-1}$，反之，任取 $ha^{-1}\in Ha^{-1}$，则 $(ha^{-1})^{-1}=ah^{-1}\in aH$。

6．设 G 有真子群，其阶应为素数的真因子，矛盾。

7．$a(H_1\cap H_2)=\{ah\mid h\in H_1\cap H_2\}=aH_1\cap aH_2$。

8．任取 $a\neq e$，$\langle a\rangle$是子群，其阶为 p^n 的因子，即为 $p^l(l\leqslant n)$．取 $b=a^{p^{l-1}}$，则 $b^p=a^{p^l}=e$，且 $b\neq e$（由 a 的阶为 p^l 保证）．故 b 为 p 阶元。

9．左陪集为$\{(x,x)\mid x\in R^*\}$，右陪集为$\{(x,1)\mid x\in R^*\}$。

10．子群 5 个：$\{a\}$，$\{a,b\}$，$\{a,c\}$，$\{a,d\}$，B_4。

11．$G=H\cup aH=Ha\cup H$，$(a\notin H)$．$aH=G\setminus H=Ha$。

习题 3·5

1．设 $C_n=\langle a\rangle$，$\frac{n}{d}=k$，则 $\langle a^k\rangle$ 是 d 阶子群。

2．设 σ 是 $\langle a\rangle$ 到 G 的满同态，则 $G=\langle\sigma(a)\rangle$。

3．设 $q=\frac{n}{m}$，解为 a^q，a^{2q}，…，$a^{(m-1)q}$，a^n。

4．(1) $\{e\}$；(2) 素数阶群。

5．若 G 有 n 阶元 a，则 $\langle a\rangle=\{a,a^2,\cdots,a^n\}=G$，$G$ 是循环群。反之，若 G 是循环群 $\langle a\rangle$，则 a 是 n 阶元。设 $|G|=p$，任取 $a\in G$，$a\neq e$，a 的阶是 p 的因子，又非 1，故为 p，$G=\langle a\rangle$。

6．设 $H=\langle a\rangle$，$K=\langle b\rangle$，则 $(ab)^{rs}=a^{rs}b^{rs}=e$。若 $(ab)^m=e$，则 $a^mb^m=e\in\langle a\rangle$，$b^m\in\langle a\rangle$，所以 $(b^m)^r=e$，$b^{mr}=e$，即 $s\mid mr$，由于 $(r,s)=1$，故 $s\mid m$。同理可证 $r\mid m$，即 $rs\mid m$。总之．ab 的阶为 rs。

7．若 $(m,n)=d\neq1$，设 $m=dm_1,n=dn_1$，$(a^m)^{n_1}=a^{nm_1}=e$，故 $\langle a^m\rangle\neq\langle a\rangle$。反之，若 $(m,n)=1$，则 $a^m,a^{2m},\cdots,a^{nm}$ 互不相同，即 $\langle a^m\rangle=\langle a\rangle$。

8．假若 $\mathbf{Z}[i]=\langle a+bi\rangle$，则 $i\in\langle a+bi\rangle$，设 $i=n(a+bi)=na+nbi$，则 $na=0$，$nb=1$，故 $a=0$。$1\in\langle a+bi\rangle$，设 $1=m(a+bi)=ma+mbi$，则 $mb=0,b=0$，得到 $a+bi=0$。矛盾。

习题 3·6

1．n 阶群同构于 n 元集的一个变换群，而后者只能是有限个，因为它们是 n 元集一一变换群的子群。

2. $D_4, \{R_{2\pi}\}, \{R_{2\pi}, R_\pi, D_1, D_2\}, \{R_{2\pi}, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3}{2}\pi}\}$,
$\{R_{2\pi}, H, V, R_\pi\}$, $\{R_{2\pi}, D_1\}, \{R_{2\pi}, D_2\}, \{R_{2\pi}, R_\pi\}, \{R_{2\pi}, H\}$,
$\{R_{2\pi}, V\}$。

3. D_4; $\{R_{2\pi}, R_\pi, D_1, D_2\}$; $\{R_{2\pi}, H, V, R_\pi\}$; $\{R_{2\pi}, H, V, R_\pi\}$。

4. $R_{\frac{\pi}{2}}, R_\pi = (R_{\frac{\pi}{2}})^2, R_{\frac{3}{2}\pi} = (R_{\frac{\pi}{2}})^3, R_{2\pi} = (R_{\frac{\pi}{2}})^4$, H, $V = (R_{\frac{\pi}{2}})^2 \cdot H, D_1 = R_{\frac{\pi}{2}} \cdot H, D_2 = (R_{\frac{\pi}{2}})^3 \cdot H$。

5. 用 T_a 表示这种变换的集合。$\varepsilon_A \in T_a \neq \phi$，设 σ，$\tau \in T_a$，则 $\sigma\tau(a) = \sigma(\tau(a)) = \sigma(a) = a, \sigma\tau \in T_a$。由于 σ 是一一变换，$\sigma(a) = a$，故 $\sigma^{-1}(a) = a$，$\sigma^{-1} \in T_a$。

6. 设 $\langle a\rangle = C_n$，任取 $a^k \in \langle a\rangle$，作左乘变换 σ_{a^k} 如下：$\sigma_{a^k}(a^m) = a^k \cdot a^m = a^{k+m}$。$a^k \to \sigma_{a^k}$ 是 C_n 的正则实现。

7. 任取 $n \in \mathbf{Z}$，作左加变换 σ_n 如下：$\sigma_n(m) = n + m$。$n \to \sigma_n$ 是 $\langle \mathbf{Z}, +\rangle$ 的正则实现。

8. 不。无单位元。

9. σ_1, σ_4。无右零元。

10. $\tau_{(a,b)}$ 是 $\mathbf{R}$ 的一一变换。$(\tau_{(c,d)} \cdot \tau_{(a,b)})(x) = \tau_{(c,d)}(\tau_{(a,b)}(x)) = \tau_{(c,d)}(ax + b) = c(ax + b) + d = cax + cb + d$。$\tau^{-1}_{(a,b)}(x) = \dfrac{1}{a}x - \dfrac{b}{a}$，$\varepsilon = \tau_{(1,0)}$。所以全体 $\tau_{(a,b)}$ 作成 $\mathbf{R}$ 的变换群。令 $\tau_{(a,b)} \to (a, b)$，可证与§3·1例5的群反向同构。

习题 3·7

1. (1) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$.

2. (1), (1 2 3),(1 3 2), (1 3 4), (1 4 3),(1 2 4), (1 4 2), (2 3 4),(2 4 3),(1 2)(3 4),(1 3)(2 4),(1 4)(2 3).

3. (1 5 3)(2 8 6);(1 2 3 7 4)(5 6).

4. (1) 化为(1 2)(3 7 4 5 6). 阶为[2, 5] = 10.(2)阶为[4,2,2] = 4;(3)化为不相交循环之积:(1 2 4 3 5 6)阶为6.(4). 化为(2 3 5 4), 阶为4.

5. (1) 化为(1 2 4 3 5) = (1 5)(1 3)(1 4)(1 2);(2) 化为(1 3 4) = (1 4)(1 3).

7. {(1),(1 3 2),(1 2 3)}.

8. 设$i<j-1$, 则$(i, j)=(j, j-1)\cdots(i+2, i+1)(i, i+1)(i+1, i+2)\cdots(j-1, j)$. 利用定理 4.

9. $\pi\pi^{-1}=[(s_1s_2\cdots s_t)\cdots(j_1j_2\cdots j_n)(i_1i_2\cdots i_k)][(i_k\cdots i_2i_1)(j_n\cdots j_2j_1)\cdots(s_t\cdots s_2s_1)]=(1)$. 同理$\pi^{-1}\pi=(1)$.

10. $\pi(1)\xrightarrow{\pi^{-1}}1\xrightarrow{(1\ 2\ \cdots r)}2\xrightarrow{\pi}\pi(2)$.

习题 3·8

1. 利用习题 3·4 第 11 题.

2. A_n在S_n中指数为 2. 利用上题.

3. 左陪集有: B_4, (2 3 4)B_4 = {(2 3 4),(1 3 2), (1 4 3), (1 2 4)}, (2 4 3)B_4 = {(2 4 3), (1 4 2),(1 2 3),(1 3 4)}, 右陪集也是以上三个, 故B_4是A_4的正规子群.

4. 设N_1, N_2是G的正规子群，任取$g\in G$, $n_1\in N_1$, $n_2\in N_2$，则$gn_1n_2g^{-1}=gn_1g^{-1}gn_2g^{-1}\in N_1N_2$，故$N_1N_2$是正规子群。任取$g\in G$, $n\in N_1\cap N_2$，则$gng^{-1}\in N_1$, $gng^{-1}\in N_2$, $gng^{-1}\in N_1\cap N_2$，故$N_1\cap N_2$是G的正规子群。

5. 不一定。如B_4是A_4的正规子群，而$\{(1), (1\ \ 2)(3\ \ 4)\}$是$B_4$的正规子群(指数为2)，但$\{(1), (1\ \ 2)(3\ \ 4)\}$不是$A_4$的正规子群$(1\ \ 2\ \ 3)$的左陪集为$\{(1\ \ 2\ \ 3), (1\ \ 3\ \ 4)\}$，右陪集为$\{(1\ \ 2\ \ 3), (2\ \ 4\ \ 3)\}$。

6. 设N是群G的子群，任取$g\in G$,则gNg^{-1}仍是子群，且与N同阶，由于与N同阶的子群只有N，则$gNg^{-1}=N$,故N是正规子群。

7. 任取$n\in H\cap N$, $h\in H$，则$hnh^{-1}\in h$, $hnh^{-1}\in N$,即$hnk^{-1}\in H\cap N$。$H\cap N$是H的正规子群。$HN=\{hN|h\in H\}=\{Nh|h\in H\}=NH$，因而$HN$是子群。

8. $a=e^{-1}ae$,故$a\sim a$;若$a\sim b$,则有$g\in G$,使$a=g^{-1}bg$, $b=(g^{-1})^{-1}ag^{-1}$, $b\sim a$; 若$a\sim b$, $b\sim c$，则有g, $h\in G$，使$a=g^{-1}bg$, $b=h^{-1}ch$, $a=(hg)^{-1}c(hg)$，即$a\sim c$。

9. 正规子群：(1)，A_3，S_3。中心：(1)。

10. 设$\langle a^k\rangle$是$\langle a\rangle$的任一子群，则$\langle a\rangle/\langle a^k\rangle=\{\langle a^k\rangle, a\cdot\langle a^k\rangle, \cdots, a^{k-1}\cdot\langle a^k\rangle\}=\langle a\cdot\langle a^k\rangle\rangle$作成$k$阶循环群，生成元为$a\cdot\langle a^k\rangle$。

11. 设C_1是中心C的子群,任取$g\in G$，则对于$c_1\in C_1$，有$gc_1g^{-1}=c_1gg^{-1}=c_1\in C_1$故$C_1$是正规子群。

12. D_4，$\{R_{2\pi}\}$以及所有四阶子群。

13. N是正规子群$\Longleftrightarrow$对于$g\in G$，$gN=Ng\Longleftrightarrow gNg^{-1}=N$。

习题 3·9

1．设 a 为 n 阶，σ 为同态，则 $\sigma(a)^n=\sigma(a^n)=\sigma(e)=\bar{e}$.

2．(2) 是，$k_\varphi=\{1,-1\}$，$\varphi[\boldsymbol{R}^*]=\boldsymbol{R}^+$；(3) 是，$k_\varphi=\langle n\rangle$，$\varphi[\boldsymbol{Z}]=\boldsymbol{Z}_n$；(4) 是，$k_\varphi=\{[2],[4],[6],[0]\}$，$\varphi[\boldsymbol{Z}_8]=\boldsymbol{Z}_2$.

3．由 § 3·7 定理 6 得证．核为 A_n.

4．若 C_n 与 C_m 同态，则 $|C_m|$ 整除 $|C_n|$，即 $m|n$. 反之，若 $m|n$，$\dfrac{n}{m}=d$，$C_n=\langle a\rangle$，$C_m=\langle b\rangle$，作映射 $a^{kd+r}\to b^r$，$k=0,1,\cdots,m-1$. $r=0,1,\cdots,d-1$，是 $\langle a\rangle$ 到 $\langle b\rangle$ 的同态满射.

5．$\varphi(n+m)=a^{n+m}=a^n\cdot a^m=\varphi(n)\cdot\varphi(m)$. $K_\varphi=\langle n\rangle$（$n$ 为 a 的阶），$\varphi[\boldsymbol{Z}]=\langle a\rangle$.

6．任取 $r(\cos\theta+i\sin\theta)\in\boldsymbol{C}^*$，映射 $r(\cos\theta+i\sin\theta)\to r$ 是 $\langle\boldsymbol{C}^*,\cdot\rangle$ 到 $\langle\boldsymbol{R}^+,\cdot\rangle$ 的满同态，核为 W.

习题 3·10

1．设 $\bar{H}=\varphi[H]$，$\bar{H}$ 是 $\bar{G}$ 的子群，$\varphi^{-1}[\bar{H}]$ 是 G 的子群，且 $\varphi[\varphi^{-1}[\bar{H}]]=\bar{H}$，由此可知，$\varphi^{-1}[\bar{H}]$ 与 $\bar{H}$ 同态.

2．由第二同构定理，$HN/N\cong H/H\cap N=H/\{e\}\cong H$.

3．作 G/K 到 G/H 的映射 φ：$\varphi(gK)=gH$. 其核为 $\{hK\mid h\in H\}=H/K$，φ 是同态．由同态基本定理得证.

4．$S_4=S_3B_4$，$S_3\cap B_4=(1)$．由第二同构定理：$S_4/B_4=S_3B_4/B_4\cong S_3/S_3\cap B_4\cong S_3$.（至于 B_4 是 S_4 的正规子群，另外证明）

5. $\langle a^n\rangle\cdot\langle a^m\rangle=\langle a^d\rangle$, $\langle a^n\rangle\cap\langle a^m\rangle=\langle a^l\rangle$. 由第二同构定理，$\langle a^d\rangle/\langle a^n\rangle\cong\langle a^m\rangle/\langle a^n\rangle\cap\langle a^m\rangle=\langle a^m\rangle/\langle a^l\rangle$.

6. 首先证明 $K'(K\cap L')$ 是 $K'(K\cap L)$ 的正规子群，然后利用第二同构定理，取 $H=K\cap L$, $N=K'(K\cap L')$, 得

$K'(K\cap L')(K\cap L)/K'(K\cap L')\cong(K\cap L)/(K\cap L)\cap K'(K\cap L')$；证明它可化为

$$K'(K\cap L)/K'(K\cap L')$$
$$\cong(K\cap L)/(K'\cap L)(K\cap L').$$

习题 3·11

1. 自同态：σ_1, σ_2, σ_4. 自同构：σ_1, σ_2.

2. (1) 由于 φ 和 φ^{-1} 都是自同态，a 与 $\varphi(a)$ 的阶互不超过(习题 3·9—1).

3. $C_\infty\cong\langle \boldsymbol{Z},+\rangle$, 由 § 2·4 例 3 $\langle \boldsymbol{Z},+\rangle$ 的自同态形如 $n\to pn$, p 为任意整数. 所以其自同态半群为 $\langle \boldsymbol{Z},\cdot\rangle$. 由习题 2·4—8 结果，$\langle \boldsymbol{Z},+\rangle$ 的自同构只有两个($p=\pm1$)，所以自同构群为 $\langle\{1,-1\},\cdot\rangle$.

4. 若 G 为可换群，则 $\sigma(ab)=(ab)^{-1}=b^{-1}a^{-1}=a^{-1}b^{-1}=\sigma(a)\sigma(b)$, σ 为同态，且是一一映射，故为同构. 反之，若 σ 为自同构，则 $\sigma(a^{-1}b^{-1})=\sigma((ba)^{-1})=ba$, $\sigma(a^{-1}b^{-1})=\sigma(a^{-1})\sigma(b^{-1})=ab$, 即 $ab=ba$, G 为可换群.

5. 见 § 3·1 例 4. 每个自同构使单位元 a 保持不变. b, c, d 为二阶元，每个自同构相当于 $\{b, c, d\}$ 的一个排列，共 $3!=6$ 个自同构. 与 S_3 一一对应，且运算保持一致.

6. H 是正规子群 $\Longleftrightarrow$ 对任意 $g\in G$, $gHg^{-1}=H\Longleftrightarrow H$ 在任意内自同构下不变.

7. 若G不是可换群，设$ab\neq ba$，则$aba^{-1}\neq b$. $x\to axa^{-1}$是自同构，但不是恒等变换. 矛盾. 如有$a\in G$, $a^2\neq e$，则$x\to x^{-1}$是G的一个自同构，它不是恒等变换($a\neq a^{-1}$)，矛盾.

8. 必要性：若a是φ的不动元，则$a=\varphi(a)$，$a\to\varphi(a)a^{-1}=aa^{-1}=e$，而$e\to\varphi(e)e^{-1}=ee^{-1}=e$，故$a=e$. 充分性：若$\varphi(a)a^{-1}=\varphi(b)b^{-1}$，则$a^{-1}b=\varphi(a)^{-1}\varphi(b)=\varphi(a^{-1}b)$，即$a^{-1}b$是$\varphi$的不动元，因而$a^{-1}b=e$，$a=b$，$a\to\varphi(a)a^{-1}$为单射.

习题 3·12

1. $\bar{G}_1$显然是G的子群. 任取$a_1\in G_1$, $a_2\in G_2$，则$(a_1, a_2)\bar{G}_1(a_1, a_2)^{-1}=(a_1, a_2)\bar{G}_1(a_1^{-1}, a_2^{-1})=\{(a_1g_1a_1^{-1}, a_2e_2a_2^{-1})|g_1\in G_1\}=\{(a_1g_1a_1^{-1}, e_2)|g_1\in G_1\}\subseteq\bar{G}_1$，故$\bar{G}_1$是$G$的正规子群. $g_1\to(g_1, e_2)$是G到$\bar{G}_1$的同构. 作G到$\bar{G}_2$的映射：$(g_1, g_2)\to(e_1, g_2)$. 它是同态，核为$\bar{G}_1$，因而$G/\bar{G}_1\cong\bar{G}_2$. 其他结论类似可得.

2. 设C_1, C_2是G_1, G_2的中心. 任取$c_1\in C_1$, $c_2\in C_2$, $g_1\in G_1, g_2\in G_2$，则$(g_1,g_2)(c_1,c_2)=(g_1c_1,g_2c_2)=(c_1g_1,c_2g_2)=(g_1, g_2)(c_1,c_2)$，$(c_1,c_2)\in G_1\times G_2$的中心. 反之，设$(c_1, c_2)\in G_1\times G_2$的中心，可推出$c_1\in C_1$, $c_2\in C_2$.

3. 任取$(a,b)\in G_1\times G_2$，$(a,b)\to(b,a)$是同构映射.

4. 不. C_{60}有四阶元，而$C_{10}\times C_6$无四阶元.

5. 不. D_4不可换. 而$C_4\times C_2$可换.

6. $625=5^4=5\cdot5\cdot5\cdot5=5\cdot5\cdot5^2=5^3\cdot5=5^2\cdot5^2$ 故625阶可换群共有五个同构类：$C_{625}, C_5\times C_5\times C_5\times C_5, C_5\times C_5\times C_{25}$, $C_{125}\times C_5$, $C_{25}\times C_{25}$.

7. $120=2^3\cdot3\cdot5=2^2\cdot2\cdot3\cdot5=2\cdot2\cdot2\cdot3\cdot5$，故120阶可换群共有三个同构类：$C_8\times C_3\times C_5$，$C_4\times C_2\times C_3\times C_5$，$C_2\times C_2\times C_2\times C_3\times C_5$。

8. (1)、(2)不可分解，$C_{111}\cong C_3\times C_{37}$，$C_{527}\cong C_{17}\times C_{31}$。

9. S_3不是循环群，故其生成系至少含两个元素．而$(1)=(1\ 2)^2$，$(1\ 3)=(1\ 2\ 3)(1\ 2)$，$(2\ 3)=(1\ 2)(1\ 2\ 3)$，$(1\ 3\ 2)=(1\ 2\ 3)^2$．故$\{(1\ 2),(1\ 2\ 3)\}$作成S_3的最小生成系。

习题 3·13

1. $\{(1)\}$，$\{(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$。

2. 设N是正规子群，$g\in N$，其共轭元形如$h=aga^{-1}\in N$。反之，若$g\in N$，任取$a\in g$，则aga^{-1}是g的共轭元，故属于N，因而N是正规子群．

3. 若a与b共轭，则b是a在某内自同构下的象．因而a，b同阶(习题3·11—2)．

4. 设$b=gag^{-1}$，$b^{-1}=(gag^{-1})^{-1}=ga^{-1}g^{-1}$．$b^n=(gag^{-1})^n=gag^{-1}gag^{-1}\cdots gag^{-1}=ga^ng^{-1}$，$b^0=e=ga^0g^{-1}$，$b^{-n}=(b^{-1})^n=(ga^{-1}g^{-1})^n=ga^{-n}g^{-1}$ $(n>0)$．

5. 任取$\langle S\rangle$的元素$s_1s_2\cdots s_n$，任取$g\in G$，则$g(s_1s_2\cdots s_n)g^{-1}=(gs_1g^{-1})(gs_2g^{-1})\cdots(gs_ng^{-1})$是$S$的元素的共轭元之积，因而属于$\langle S\rangle$．

6. $3200=2^7\cdot5^2$．西洛2—子群为2^7阶．

7. 西洛3—子群为3阶，如$\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$。

8. 第一、三方阵共轭。

9. p 群的商群的阶应为群阶 p^n 的因子.

10. 若 G 为 p 群，阶为 p^n，则其真子群的阶为 p^n 的因子，因而也是 p 群. 反之，若有限群 G 的真子群是 p 群，而 G 不是 p 群，则有素数 $q \mid |G|$，$(q \neq p)$，由西洛定理，G 有 q 阶子群，矛盾.

11. 由西洛定理，存在 p 阶子群，它是循环群 $\langle a\rangle$，同理存在 q 阶循环子群 $\langle b\rangle$. $a^p = e$，$b^q = e$，$(ab)^{pq} = a^{pq}b^{pq} = e$. 若 $(ab)^m = e$，则 $a^m b^m = e \in \langle a\rangle$，$b^m \in \langle a\rangle$，$(b^m)^p = e$，$q \mid mp$，$q \mid m$. 同理，$p \mid m$，$pq \mid m$. 即 ab 阶为 pq，$G = \langle ab\rangle$.

12. 西洛定理中取 $k = 1$.

13. $10 = 10$，$10 = 5 + 5$，$10 = 2 + 2 + 2 + 2 + 2$，$10 = 1 + 2 + 2 + 5$.

复习题三

1. 一阶：$\{e\}$；二阶：C_2；三阶：C_3；四阶：C_4，B_4；五阶：C_5.

2. $(a \circ b) \circ c = au^{-1}bu^{-1}c = a \circ (b \circ c)$，单位元为 u，a 的逆元为 $ua^{-1}u$.

3. $1 = p^0 q^0 \in G$，G 关于乘法封闭，$(p^m q^n)^{-1} = p^{-m} q^{-n} \in G$，$G$ 是 $\langle Q^*, \cdot\rangle$ 的子群.

4. $(x^{-1}yx)^k = x^{-1}yxx^{-1}yx \cdots x^{-1}yx = x^{-1}y^k x$.

5. 见上题.

6. 设元素的阶有上界 m. 取 r_k 为 k 阶元素的个数 $(k \leqslant m)$，则 $r_1 + r_2 + \cdots + r_m = |G| < \infty$.

7. (1) 设 a, b 阶为 m 因子，则 $(ab)^m = a^m b^m = e$，即 ab 的阶是 m 因子，a^{-1} 阶与 a 相同，e 的阶为 1，故所述元素

作成子群。(2) 设 $a,b\in G$，$a^m b^m=(ab)^m$，$(a^m)^{-1}=(a^{-1})^m$，$e^m=e$。所有元素的 m 次幂作成子群。

8. 因 $e^n=e$，故 $e\in H\neq\phi$。设 $h_1,h_2\in H$，$x_1{}^n=h_1,x_2{}^n=h_2$，则 $(x_1x_2)^n=h_1h_2\in H$。$(x_1{}^{-1})^n=(x_1{}^n)^{-1}=h_1{}^{-1}\in H$。故 H 为子群。

9. $a^k,a^{2k},\cdots,a^{n_1k}=e$ 是 n_1 个互异元素。其中 $n_1=\dfrac{n}{(k,n)}$ (n_1k 是 n 的倍数)。

10. 设 $k=qn+r\ (0\leqslant r<n)$，则 $a^k=(a^n)^q\cdot a^r$，而 $a^k=e\in H,a^n\in H$，故 $a^r\in H$，$r=0$，$n|k$。在 G/H 中，$aH,a^2H,\cdots,a^{n-1}H$ 都不等于 H，而 $a^nH=H$，故 aH 阶为 n。

11. 若 G/C 是循环群，设生成元为 aC，则 $G/C=\{C,aC,a^2C,\cdots\}$，任取 $x,y\in G$，设 $x\in a^kC,y\in a^lC$，$x=a^kc_1$，$y=a^lc_2$，$xy=a^kc_1a^lc_2=a^{k+l}c_1c_2=a^lc_2a^kc_1=yx$，($c_1,c_2\in C$，故以上各因子可换) 与 G 是不可换群矛盾。由于群的内自同构群同构于 G/C，所以不是循环群，因而自同构群也不是循环群。

12. 由 §3·13 定理 2，$|N_x|\cdot k=n$，$k=\dfrac{n}{|N_x|}$，而 $\langle x\rangle=\{x,x^2,\cdots,x^m\}\subseteq N_x$，$m\,\big|\,|N_x|$，$k\,\Big|\,\dfrac{n}{m}$。

13. $k=\dfrac{n}{|N_a|}$(a 为共轭类中任一元)，而 C 是 N_a 的子群，$c\,|\,|N_a|$，故 $k\,\Big|\,\dfrac{n}{c}$。

14. 只须证明群与其中心重合。设中心为 C，由 §3·13 定理 3，$|C|=p$ 或 p^2。若 $|C|=p$，则 $|G/C|=p^2/p=p$ 应为循环群与 11 题矛盾，故有 $|C|=p^2$，$C=G$。

15. $xN(a)=yN(a)\Longleftrightarrow x^{-1}y\in N(a)\Longleftrightarrow(x^{-1}y)a(x^{-1}y)^{-1}=a\Longleftrightarrow yay^{-1}=xax^{-1}$.

16. a 的共轭元 $b=xax^{-1}$ 的象 $\varphi(b)=\varphi(x)\varphi(a)\varphi(x)^{-1}$ 仍与 $\varphi(a)$ 共轭.

17. τ 所在的共轭类的元素应形如 $\sigma\tau\sigma^{-1}$, $\sigma\in S_n$. $\sigma\tau\sigma^{-1}$ 将 $\sigma(i)$ 变换为 $\sigma(i)\xrightarrow{\sigma^{-1}}i\xrightarrow{\tau}\tau(i)\xrightarrow{\sigma}\sigma\tau(i)$. 即 $\sigma\tau\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ \sigma\tau(1) & \sigma\tau(2) & & \sigma\tau(n)\end{pmatrix}$. 现设 $\tau=(k_1\cdots k_r)\cdots(l_1\cdots l_s)$, 则 $\sigma\tau\sigma^{-1}=(\sigma(k_1)\sigma(k_2)\cdots\sigma(k_r))\cdots(\sigma(l_1)\sigma(l_2)\cdots\sigma(l_s))$, 仍是同样多的不相交循环的积, 反之, 与 τ 对应循环长度相同的不相交循环之积也必是其共轭元. 不妨设 $r\geqslant\cdots\geqslant s$, $(r+\cdots+s=n)$ 这称为 n 的一个划分. 每个共轭类对应一个划分, 同时, 每个划分对应一个共轭类, 不同的共轭类对应划分不同. 所以 S_n 共轭类个数与 n 的划分数相同. 后者是仅与 n 有关的函数, 记为 $p(n)$, 如 $p(2)=2, p(3)=3, p(4)=5, p(5)=7$ 等.

当 $n>2$ 时, 如果 $(1)\neq\tau\in C(S_n)$ (中心), 则 $\tau=(k_1\cdots k_r)\cdots$, $r\geqslant2$. 取 σ, 使 $\sigma\tau\sigma^{-1}=(\sigma(k_1)\cdots\sigma(k_n))\cdots\neq\tau$, 则得 $\sigma\tau\neq\tau\sigma$, 所以 $S_n(n>2)$ 中心只含 (1).

18. 设 f 是 G 的任意自同态, K 是其核, G 中包含 K 的子群与 G 的子群通过 $H\longrightarrow f[H]$ 建立一一对应 (见§3·10 一), 因而个数相同, 如果 $K\neq\{e\}$, 则 G 的子群比包含 K 的子群至少多一个, 矛盾. 所以 $K=\{e\}$, f 是自同构.

19. $\sigma(a)=a^{-1}(a\in G)$ 是 $A(G)$ 中的二阶元, 因 $\sigma^2=\varepsilon_G$. 由拉格朗日定理, $A(G)$ 若为有限群, 其阶应为 2 的倍数, 即

$A(G)$的阶若有限只能为偶数.

20. $\sigma(a)=a^3$, $\sigma(b)=b^3$, $\sigma(ab)=(ab)^3$, 因而 $a^3b^3=(ab)^3=ababab$,所以$a^2b^2=(ba)^2$.$(a^2)^2(b^2)^2=(b^2a^2)^2=((ab)^2)^2$, 即 $a^4b^4=(ab)^4$, $a(a^3b^3)b=a(ba)^3b, a^3b^3=(ba)^3$. 即 $\sigma(a)\sigma(b)=\sigma(ba)$,又因 σ 是同态, 所以 $\sigma(a)\sigma(b)=\sigma(ab)$, 又由 σ 是单射, 故 $ab=ba$.

21. 设 φ 是 G 的自同构, 但 $\varphi\neq\varepsilon_G$, 选取 $a\in G$, 使 $\varphi(a)=a'\neq a$,如果 φ 属于 $A(G)$的中心, 则 φ 与由 a 决定的内自同构 σ_a 可换. 即对于 $g\in G$, $(\sigma_a\varphi)(g)=(\varphi\sigma_a)(g)=\varphi(aga^{-1})=\varphi(a)\varphi(g)\varphi(a)^{-1}=a'\varphi(g)a'^{-1}=(\sigma_{a'}\varphi)(g)$.所以 $\sigma_a\varphi=\sigma_{a'}\varphi$, $\sigma_a=\sigma_{a'}$. 即由 a 和 a' 生成同一内自同构. 由 §3·11 定理 4 的证明, $e\neq aa'^{-1}\in C$, 与已知矛盾.

22. 结合律由 B 中乘法结合律保证. 零同态为零元, $(-\sigma)(x)=-\sigma(x)$为 σ 的负元(这里把 A、B 视为加群),可换性显然.

23. 设 $A=\langle a\rangle=C_\infty$. 设有 $A\to B$ 的同态 σ, $\sigma(a)=b\in B,\sigma(a^n)=b^n,n\in\mathbf{Z}$. 反之, 由 b 决定同态 $\sigma:\sigma(a)=b$. $\sigma\to\sigma(a)$是 $Hom(A,B)$到 B 的映射, 且显然是满射和单射, 因而是一一映射. 而$(\sigma*\tau)\to(\sigma*\tau)(a)=\sigma(a)\cdot\tau(a)$, 所以上述映射是同态, 因而是同构.

24. 任取自同态 σ, $\sigma\to\sigma(1)$是自同态群到 $\mathbf{Q}$ 的映射,这一映射是一一的, 也是同态.

25. 设 $b_1,b_2\in B$. 对于 $a\in A$,在 A 中有 x_2, 使 $x_2b_2=a$. 对于 x_2, A 中有 x_1,使 $x_1b_1=x_2$. 故 $x_1b_1b_2=x_2b_2=a$. 因而 b_1b_2 是 a 的右因子, 同理 b_1b_2 是 a 的左因子,因而 $b_1b_2\in B$. B 是子半群. 设 $x,y\in A$ 适合 $xb_2=b_1$, $b_2y=b_1$, 为了证 b_1,b_2 在

B中互相整除，只须证明 x，y 属于 B。设 $b_1t=a$，$(t\in A)$，则 $xb_2t=b_1t=a$，x 是 a 的左因子。再设 $b_2e=b_2$，$c_1b_1=e$，$b_2c_2=e$，$e,c_1,c_2\in A$。由于对任意的 $z\in A$，有 $z'\in A$，使 $z=z'b_2$，故 $ze=z'b_2e=z'b_2=z$，即 e 是A的右单位元。于是 $a=ae=ab_2c_2=ab_2ec_2=ab_2c_1b_1c_2=ab_2c_1xb_2c_2=ab_2c_1xe=ab_2c_1x$，即 x 是 a 的右因子。x 可整除A的任意元素，$x\in B$，同理 $y\in B$。B 中任意两元素互相整除，故为子群。

26。设 $c_1,c_2\in C$。任取 $a\in A$，在A中存在 x，使 $c_1=ax$。故 $c_1c_2=a(xc_2)$，即 c_1c_2 可被任意元素 a 左整除。同样可证右整除。故 $c_1c_2\in C$。假定有 $uc_2^2=c_2$，$c_2^2v=c_2$，$c_1=c_2w$，$u,v,w\in A$。于是，$uc_2=uc_2c_2v=c_2v$。$c_2(c_2v^2c_1)=(c_2^2v)(vc_1)=c_2vc_1=uc_2c_1=uc_2c_2w=c_2w=c_1$。下面证明 $y=c_2v^2c_1\in C$。事实上，对于任意的 $z\in A$，存在 u'，v'，使$c_1=u'z$，$c_2=zv'$。因而 $y=c_2v^2c_1=zv'v^2u'z$，即 z 是 y 的因子，$y\in C$。同样可证存在 $x\in C$，使 $xc_2=c_1$，因而 c_2 整除 c_1。由 c_1，c_2 的任意性，知 C 中任意两个元素互相整除，即 C 作成群。

27。(1) 必要性：若有 $\alpha,\beta\in A$，$\tau(\alpha)=\tau(\beta)$，$\sigma(\alpha)\neq\sigma(\beta)$，则对于 $\pi\in S(A)$，$\pi(\tau(\alpha))=\pi(\tau(\beta))$，$\pi\tau\neq\sigma$，$\tau$ 不是 σ 的右因子。充分性：规定一个变换 π 如下，当 $x\in\tau[A]$时，规定 $\pi(x)=\sigma(\alpha)$，其中 α 适合 $x=\tau(\alpha)$（π 的单值性由条件保证）；当 $x\overline{\in}\tau[A]$时，任意。则对于所有 $\alpha\in A$，$(\pi\tau)(\alpha)=\pi(\tau(\alpha))=\sigma(\alpha)$，即 $\pi\tau=\sigma$，

(2) 若$\sigma[A]\subseteq\tau[A]$，对 $x\in\sigma[A]$，固定一个 x'，使 $\tau(x')=x$。建立新的变换 π：若 $\sigma(\alpha)=\beta$，则令 $\pi(\alpha)=\beta'$。故 $(\tau\pi)(\alpha)=\tau(\beta')=\beta=\sigma(\alpha)$，因而 $\tau\pi=\sigma$，反之显然。

28. 由西洛定理，一定存在 q 阶子群，设 H 为 q 阶子群，又设 H_1 也是 q 阶子群，如果 $H \neq H_1$，则 $H \cap H_1 = \{e\}$（因为否则设 $a \in H \cap H_1$，$a \neq e$，则 $\langle a \rangle$ 是 q 阶子群，推得 $H = \langle a \rangle = H_1$），假定 $H = \langle b \rangle$，$H_1 = \langle c \rangle$，则显然 $b^i c^j$，$i, j = 0, 1, \cdots, q-1$，互不相同，那末 G 的阶 $\geqslant q^2 > pq$，矛盾。因而 q 阶子群唯一。任取 $g \in G$，gHg^{-1} 也是 q 阶子群，因而等于 H，所以 H 是正规子群。

29. 任取 $a \in G$，$aN_1N_2a^{-1} = aN_1a^{-1}aN_2a^{-1} \subseteq N_1N_2$。所以 N_1N_2 是正规子群，显然包含 N_1 和 N_2。又显然包含 N_1 和 N_2 的正规子群一定包含 N_1N_2。

30. 设 $G = \bigcup_{i=1}^{\infty} H_i$，如果 G 有非平凡正规子群 N，显然一定有某个 H_k，使 $H_k \supset H_k \cap N \neq \{e\}$。由 §3·10 引理 1，$H_k \cap N$ 是 H_k 的非平凡正规子群，推出矛盾。

习题 4·1

1. (1)、(3)、(5)是环。

4. 不。$c \cdot (b + b) = c \cdot c = c \neq b = c + c = c \cdot b + c \cdot b$。

习题 4·2

1. 可逆元：[1],[3],[7],[9],[11],[13],[17],[19]；

零因子：[2]，[4]，[5]，[6]，[8]，[10]，[12]，[14]，[15]，[16]，[18]。

2. [1]，[5]，[7]，[11]，[13]，[17]，[19]，[23]是可逆元，其他非零元是零因子。

3. 不. 设 $f_1(x)=\begin{cases}1, & \text{当 } x\in\left[0,\frac{1}{2}\right),\\ 0, & \text{当 } x\in\left[\frac{1}{2},1\right];\end{cases}$

$f_2(x)=\begin{cases}0, & \text{当 } x\in\left[0,\frac{1}{2}\right),\\ 1, & \text{当 } x\in\left[\frac{1}{2},1\right].\end{cases}$ 则 $f_1\neq 0, f_2\neq 0$,

但 $f_1f_2=0$.

4. 设 $x^2=x$, 则 $x(x-1)=0$, $x=0$ 或 $x=1$. 设 $x^n=0$, 即 $x\cdots x=0$. 若 $x\neq 0$, 推得 $x^n\neq 0$, 矛盾. 因而 $x=0$.

5. 若 $ba\neq 0$, $a(ba)=aba=0$, 说明 a 是左零因子; 否则, 设 $ab=0$, 说明 a 是右零因子.

6. $\mathbf{Z}_2$, $\mathbf{Z}_{11}$, $\mathbf{Z}_{17}$, $\mathbf{Z}_{101}$.

8. 任取非零元 a,b. 设 a 为 n 阶, 则 $0=(na)b=a(nb)$, 因而 $nb=0$, b 的阶$\leqslant n$. 同理, a 的阶$\leqslant b$ 的阶, 故 a 的阶 $=b$ 的阶.

9. 可逆元形如 $\pm\frac{2^k}{2^n}=\pm 2^s(s\in\mathbf{Z},\ k,n\in\mathbf{N})$.

11. 设 R 是有限整环, 则 R^*是有限半群且适合消去律, 由 § 3·2 定理 9, R^*是群, R 是域.

12. [23].

13. $\varphi(p)=p-1$, 由费马定理 $a^{p-1}\equiv 1(\bmod p)$.

14. 设 $\langle R,+\rangle=\langle a\rangle$. 任取 na, $ma\in R$, 则有 $na\cdot ma=(nm)a^2=ma\cdot na$.

15. 设 $(k,n)=d\neq 1$, 则 $[k]\cdot[n_1]=[k_1n]=[0]$, 其中 k_1

$=\frac{k}{d}$, $n_1=\frac{n}{d}$; $[k]$是零因子. 反之，设$[k]$是零因子，则有$[r]\neq[0]$(假定 k, r 是 0 与 n 之间的数), $[k][r]=[kr]=[0]$, $n|kr$. 若 n,k 互素，则 $n|r$, 矛盾，故$(n,k)\neq1$.

习题 4·3

1. 任取 $r\in R$, $r=r\cdot1\in I$, 故 $R=I$.

2. 设 a 是可逆元，$a\in I$, 则 $1=a^{-1}a\in I$, 由上题，$I=R$.

4. 任取 $r\in R$, $x\in I_a$, 则 $a(rx)=(ax)r=0$, $rx\in I_a$, 同理 $xr\in I_a$. 又显然 I_a是 R 的子环. 故 I_a是理想.

5. $\{[0]\}$, $\{[0], [6]\}$, $\{[0], [3], [6], [9]\}$, $\{[0], [4], [8]\}$, $\{[0], [2], [4], [6], [8], [10]\}$, $\mathbf{Z}_{12}$.

6. 设幂零元集为 N. $O\in N\neq\phi$. a_1, $a_2\in N$, $a_1^n=0$, $a_2^m=0$, $(a_1-a_2)^{m+n}=a^{m+n}-C_{m+1}^1a_1^{m+n-1}a_2+\cdots+(-1)^{m+n}a_2^{m+n}=0$. $(a_1\cdot a_2)^{m+n}=a_1^{m+n}\cdot a_2^{m+n}=0$, 故 N 是子环. 任取 $r\in R$, $(ra_1)^n=r^na_1^n=0$. N 为理想.

7. 全环.

8. 设 I 是 $\mathbf{Z}$ 的任一真理想. a 是 I 中最小正整数，则 $I=\langle a\rangle$. 否则有 $b\in I, a\nmid b$, 则有 r 满足 $0<r<a, b=qa+r$, $r=b-qa\in I$, 与 a 的取法矛盾. 此外，$\mathbf{Z}$ 的平凡理想显然是主理想$\langle0\rangle$, $\langle1\rangle$.

9. (1)设$f(x)\in$左集，则是 x^2-1 和$(x+1)^2$ 的公倍式，因而是 $(x+1)^2(x-1)$ 的倍式. 反之，设 $f(x)\in$右集，则 $f(x)$是 x^2-1 和$(x+1)^2$ 的公倍式. (2) 左集$=\{u(x)(x^2-1)+v(x)(x+1)^2|u(x), v(x)\in\mathbf{R}[x]\}=\langle x+1\rangle$. (由 $x+1$ 是

x^2-1 与 $(x+1)^2$ 的最大公因式得出)

10. $|R|\geqslant 2$. $r^2-r=r(r-1)=0$, $r=0,1$. 故 $|R|=2$.

11. $0\in I\neq\phi$, 任取 $r\in R$, $a,b\in I$, 设 $a\in I_n$, $b\in I_m$, $n\leqslant m$, $a-b\in I_m\subseteq I$. $ra\in I_n\subseteq I$, $ar\in I$.

12. 只须证明加法交换律: $a+a+b+b=(1+1)a+(1+1)b=(1+1)(a+b)=1(a+b)+1(a+b)=a+b+a+b$. 两端约去 a 和 b, 得 $a+b=b+a$.

习题 4·4

1. R 的性质如结合律、交换律、分配律、有零元和负元等可由 φ 传递到 $\bar{R}$ 中.

2. 若 $\varphi(u)$ 可逆, 则 $\varphi(u)\neq\bar{0}$, $u\in K_\varphi$. 反之, 若 $u\in K_\varphi$, 则 $\varphi(u)\neq\bar{0}$, $\phi(u)\phi(u^{-1})=\phi(uu^{-1})=\phi(1)=\bar{1}$.

4. $\varphi_1([n])=[0]$;

$$\varphi_2:\begin{cases}[0],\ [3],\ [6],\ [9],\ [12]\to[0]\in\mathbf{Z}_3,\\ [1],\ [4],\ [7],\ [10],[13]\to[1]\in\mathbf{Z}_3,\\ [2],\ [5],\ [8],\ [11],[14]\to[2]\in\mathbf{Z}_3.\end{cases}$$

5. $\varphi_1([n])=[0]$.

6. (1) 设同态为 φ, S 是 R 的子环, $\varphi[S]=\bar{S}$, 任取 $\varphi(s_1)$, $\varphi(s_2)\in\bar{S}$, 则 $\varphi(s_1)-\varphi(s_2)=\varphi(s_1-s_2)\in\bar{S}$, $\varphi(s_1)\varphi(s_2)=\varphi(s_1s_2)\in\bar{S}$, 故 $\bar{S}$ 是 $\bar{R}$ 的子环. 若 S 又是理想, 任取 $\varphi(r)\in\bar{R}$, 则 $\varphi(r)\varphi(s_1)=\varphi(rs_1)\in\varphi[S]=\bar{S}$, $\varphi(s_1)\varphi(r)\in\bar{S}$. $\bar{S}$ 是理想. (2) 设 $\bar{S}$ 是 $\bar{R}$ 的子环, $\varphi^{-1}[\bar{S}]=S$. 任取 s_1, $s_2\in S$, $\varphi(s_1-s_2)=\varphi(s_1)-\varphi(s_2)\in\bar{S}$, $\varphi(s_1s_2)=\varphi(s_1)\varphi(s_2)\in\bar{S}$. s_1s_2, $s_1-s_2\in\varphi^{-1}[\bar{S}]=S$. 若 $\bar{S}$ 又是理想, 任取 $r\in R$, 则 $\varphi(rs_1)=\varphi(r)\varphi(s_1)\in\bar{S}$,

$rs_1 \in S$，同理 $s_1 r \in S$。S 是理想。

习题 4·5

1．(1) $[4]x^4+[2]x^3-[4]x^2-[3]x+[4]$；(2) $[3]x^3+[1]x^2-[1]x+[2]$。

2．(1) 是，$4x-3$；(2) 是，x^2-2；(3) 是，设 $\sqrt{3}+\sqrt{5}=\alpha$，则 $\alpha^2=8+2\sqrt{15}$，$(\alpha^2-8)^2=\alpha^4-16\alpha^2+64=60$，故 α 是 x^4-16x^2+4 的根。(4) 不是。

3．商式 $=[2]x$，余式 $=-[1]x+[2]$。

4．$[0],[4]$。

5．$([1]x-[1])^3([1]x+[1])$。

6．$\sigma(f(x)+g(x))=f(0)+g(0)=\sigma(f(x))+\sigma(g(x))$，$\sigma(f(x)g(x))=f(0)g(0)=\sigma(f(x))\sigma(g(x))$。$\sigma$ 是环同态。K_σ 等于一切不含零次项的多项式的集合。

7．$R[x]$ 的可逆元是且仅是 R 的可逆元。

8．$([3]x^2-[1]x+[1])+I$ 与 $([2]x-[1])+I$ 之积等于 $([1]x^3+[3]x-[1])+I=[([3]x^2+[3]x+[2])([2]x+[3])+[3]]+I=[3]+I$。

习题 4·6

1．(1)、(2)、(4)、(6)、(7) 是既约元。

2．$2\cdot 2\cdot(x^2-x+2)$。

3．设 $k\in(a_1,b_1)$，则 $kd\mid a$，$kd\mid b$，$kd\mid d$，d 与 kd 相伴，k 是可逆元，a_1 与 b_1 互素。

4．$N(\alpha\beta)=|\alpha\beta|^2=|\alpha|^2|\beta|^2=N(\alpha)N(\beta)$。$\mathbf{Z}[i]$ 的可逆元是 ±1，$\pm i$（见习题 2·3—5）。设 $N(\alpha)=p$，$\alpha=\beta r$，$N(\alpha)$

$=N(\beta)N(r)$，则 $N(\beta)=1$ 或 p，$N(r)=p$ 或 1，设 $N(\beta)=1$，则 $\beta=\pm 1$ 或 $\pm i$，β 是可逆元，α 是既约元。

5. 设 a 为 R 非可逆的非零元，若 $R[x]$ 是主理想环，则有 $f(x)\in R[x]$，使 $\langle a, x\rangle=\langle f(x)\rangle$。$a\in\langle f(x)\rangle$，设 $a=f(x)g(x)$，从次数可见，$f(x)\in R, g(x)\in R$，令 $f(x)=b, g(x)=c$，则 $\langle a,x\rangle=\langle b\rangle$。$b$ 不是可逆元，否则 $\langle b\rangle=R=\langle 1\rangle$，存在 $u(x)$，$v(x)$，使 $u(x)a+v(x)x=1$，设 $u(x)$ 常数项为 u_0，于是 $u_0a=1$，与要求 a 非可逆元矛盾。而 $x\in\langle b\rangle$，设 $x=q(x)b, q(x)$ 形如 $hx(h\in R)$，则 $x=bhx, bh=1, b$ 可逆，矛盾。

6. 若 $7+0i$ 是可约元，等于 $\alpha\beta$，α 是真因子，$49=N(7+0i)=N(\alpha)N(\beta)$，$N(\alpha)$ 只能为 7，设 $\alpha=a+bi$，则 $a^2+b^2=7$，这样整数 a,b 不存在。

7. $([1]x^2+[2])([1]x+[2])$。

8. $\langle a,b\rangle$ 是主理想，设为 $\langle d_1\rangle$。由于 $d|a$，$d|b$，故 $\langle a, b\rangle\subseteq\langle d\rangle$，即 $\langle d_1\rangle\subseteq\langle d\rangle$。$d_1\in\langle d\rangle$，$d|d_1$，因 d_1 显然是 a,b 公因子，故 $d_1|d$，d 与 d_1 相伴，$\langle a,b\rangle=\langle d_1\rangle=\langle d\rangle$，$d\in\langle a,b\rangle=\langle a\rangle+\langle b\rangle$，存在 u,v，使 $au+bv=d$。而 a,b 互素相当于 $d=1$。

9. $au+bv=1$ 成立，$u,v\in R_1\subseteq R$。

习题 4·7

1. 素理想：$\mathbf{Z}_{12}$，$\{[0], [2], [4], [6], [8], [10]\}$，$\{[0], [3], [6], [9]\}$；最大理想同上。

2. 由于域的理想只有 $\{0\}$ 和全域，同态核只有这两种情况。

3. $\mathbf{Z}_{pq}/\langle [p]\rangle\cong\mathbf{Z}_q$ 是域。

4. 偶数环关于$\langle 4\rangle$的商环$E/\langle 4\rangle$不是域. $(2+\langle 4\rangle)^2=\langle 4\rangle=\langle 0\rangle$.

5. (1)$\langle x-1\rangle$; (2) $(x+1)+I=2+I$, $x^2-2+I=-1+I$, $(2+I)(-1+I)=-2+I$. $(2+I)^{-1}=\frac{1}{2}+I$.

6. 最大理想: $\langle 1\rangle$, $\langle i\rangle$, $\langle 1+2i\rangle$, $\langle 7\rangle$.

7. 设$a\notin H$, 令$H_1=\{h+ax|h\in H, x\in R\}$,则$H_1\supseteq H$, H_1是理想, $a^2=0+a\cdot a\in H_1$, 但因$a^2\notin H$, 故$H\subset H_1$, 由于H是最大理想, $H_1=R$. 任取$r\in R$, 则有$h\in H$, $x\in R$, $h+ax=r$, $r+H=(a+H)(x+H)$, R/H是域. 反之, 若R/H是域, $a\notin H$, 则$a+H\neq H$, $a^2+H=(a+H)(a+H)\neq H$(域无零因子, H是R/H的零元).

8. $[1]x^2+[1]$是二次多项式, 若可约必有一次因子,因而在$\mathbf{Z}_3$有根, 但显然无根, 故$[1]x^2+[1]$为既约多项式, $\mathbf{Z}_3[x]/\langle[1]x^2+[1]\rangle$是域.所求的逆元为$[2]x+[1]+\langle[1]x^2+[1]\rangle$.

复习题四

1. 若e不是右单位元, 则有$b\in R$, $be\neq b$. 于是$e+b-be\neq e$. 任取$a\in R$, $(e+b-be)a=ea+ba-bea=a+ba-ba=a$,于是$R$有另一个左单位元$e+b-be$, 矛盾.

2. 因为有c, 使$(1-ab)c=c(1-ab)=1$, 则$cab=abc=c-1$, $(1+bca)(1-ba)=1-ba+bca-bcaba=1-ba+bca-b(c-1)a=1$, $(1-ba)(1+bca)=1-ba+bca-babca=1-ba+bca-b(c-1)a=1$. 故$(1-ba)^{-1}=1+bca$.

3. $\{a+b\sqrt{2}\,|a^2-2b^2=1\}$.

4. 若 a 是可逆元，取 $b=a^{-1}$，则显然两条成立。反之，若两条件成立，则 $ab=(ba^2b)(ab)=(ba)(aba)b=(ba)ab=ba^2b=1$. $ba=(ba)(ba^2b)=b(aba)(ab)=ba(ab)=ba^2b=1$，即 $b=a^{-1}$.

5. $(p-1)^2=p^2-2p+1\equiv 1\pmod p$，其他 $k=1,2,\cdots p-2$，有 $k^2-1=(k+1)(k-1)$ 不含 p 的倍数。

6. $\mathbf{Z}_p$ 是域，$\langle \mathbf{Z}_p^*, \cdot\rangle$ 是群。除 $[1]$(1 阶元) 和 $[p-1]$(2 阶元) 之外，其他是高阶元素，两两互逆，故 $[2]\cdots[p-2]=[1]$。所以，$[(p-1)!]=[1][2]\cdots[p-2][p-1]=[1][p-1]=[p-1]=[-1]$。所以，有下式：$(p-1)!\equiv -1\pmod p$。

7. $1\in N\neq\phi$. 设 $a\in N$, a^{-1} 也是可逆元，设 $a=1+c\in 1+I$，则 $a^{-1}a=1=a^{-1}+a^{-1}c$, $a^{-1}=1-a^{-1}c\in 1+I$. 故 $a^{-1}\in N$. 设 $a,b\in N$，则 ab 是可逆元。设 $a=1+c$, $b=1+d$, $c,d\in I$，因而 $ab=1+(c+d+cd)\in 1+I$，$ab\in N$。设 R 的可逆元群为 G，任取 $g\in G$，$a\in N$，则 $gag^{-1}\in G$，且 $gag^{-1}=g(1+c)g^{-1}=1+gcg^{-1}\in 1+I$，故 $gag^{-1}\in N$。N 是 G 的正规子群。

8. 作 R/J 到 R/I 的映射如下：$r+J\rightarrow r+I$. 它是同态映射，核为集合 $\{i+J\mid i\in I\}=I/J$，因而由同态基本定理得证。

9. 设 $H=\{x+\langle a\rangle\mid x\in T_a\}$。若 x 与 a 互素，y 与 a 互素，则 xy 与 a 互素，因而 H 关于乘法封闭。任取 $x+\langle a\rangle\in H$，由 x 与 a 互素，$1\in\langle x,a\rangle$，存在 u,v，使 $ux+va=1$. $ux-1\in\langle a\rangle$，$(u+\langle a\rangle)(x+\langle a\rangle)=1+\langle a\rangle$，$u+\langle a\rangle=(x+\langle a\rangle)^{-1}$. H 是 $\langle R/\langle a\rangle, \cdot\rangle$ 的子群。

10. 设理想 $\langle b\rangle$ 含 a，则 $b\mid a$，由于 a 的既约因子除相伴外是完全确定的有限个元素，因而 a 的因子除相伴外也只有

有限个.

11. 任何 $a+bi\in\mathbf{Z}[i]$ 可写成 $a+bi=3(u+vi)+a_1+b_1i$ $(a_1, b_1=0, 1, 2)$, 因而 $\mathbf{Z}[i]/\langle 3\rangle=\{\langle 3\rangle, 1+\langle 3\rangle, 2+\langle 3\rangle, i+\langle 3\rangle, 2i+\langle 3\rangle, 1+i+\langle 3\rangle, 1+2i+\langle 3\rangle, 2+i+\langle 3\rangle, 2+2i+\langle 3\rangle\}$. 任意两个元素之积(包括自乘,但除 $\langle 3\rangle$ 外)可以验证均不为 0(即 $\langle 3\rangle$),故 $\mathbf{Z}[i]/\langle 3\rangle$ 无零因子, $\langle 3\rangle$ 是素理想. 同样可知 $\mathbf{Z}[i]/\langle 2\rangle=\{\langle 2\rangle, 1+\langle 2\rangle, i+\langle 2\rangle, 1+i+\langle 2\rangle\}$,但 $(1+i+\langle 2\rangle)^2=\langle 2\rangle$, 故有零因子.

12. $F[0,1]/F_0[0,1]\cong\boldsymbol{R}$ 是域. ($f(x)\to f(0)$ 是 $F[0,1]$ 到 $\boldsymbol{R}$ 的同态, 核为 $F_0[0,1]$).

13. 设 $P=\bigcap_{n=1}^{\infty}P_n$, P 显然是理想. 设 $ab\in P, a\overline{\in}P$, 则存在 $n>0$, 使 $a\overline{\in}P_n$, 因而当 $k\geqslant n$ 时, $a\overline{\in}P_k$. P_k 都是素理想, 所以 $b\in P_k$, $k=n$, $n+1,\cdots$, $b\in\bigcap_{n=1}^{\infty}P_n=P$.

14. $0\in S\neq\phi$. 任取 a_1, $a_2\in S$, $\sigma(a_1-a_2)=\sigma(a_1)-\sigma(a_2)=a_1-a_2$, $\sigma(a_1a_2)=\sigma(a_1)\sigma(a_2)=a_1a_2$, 即 a_1-a_2, $a_1a_2\in S$, S 为子环. 设 1 为单位元, 由 σ 不是零同态, 故 $\sigma(1)=1$, 即 $1\in S$. 任取 S 中的非零元 a, 则

$$1=\sigma(1)=\sigma(aa^{-1})=a\sigma(a^{-1}).$$

上式左乘 a^{-1}, 可得 $a^{-1}=\sigma(a^{-1})$, 即 $a^{-1}\in S$. S 为子体.

($\sigma(1)=1$ 的证明: 若 $\sigma(1)=r$, 则 $r\neq 0$, 否则 $\sigma(a)=\sigma(a\cdot 1)=\sigma(a)\cdot 0=0$, 与已知矛盾. 设 $\sigma(a)\neq 0$, 则 $\sigma(a)=\sigma(a\cdot 1)=\sigma(a)r$, 推出 $r=1$)

15. $P\cap S$ 显然是 S 的理想, 若 a, $b\in S, ab\in P\cap S$, 则 $ab\in P$, 或 $a\in P$, 或 $b\in P$, 即或 $a\in P\cap S$, 或 $b\in P\cap S$.

16. $\sigma^{-1}[P]$是理想. 若 $ab\in\sigma^{-1}[P]$, 则 $\sigma(ab)\in P$, 因而或 $\sigma(a)\in P$, 或 $\sigma(b)\in P$, 即 $a\in\sigma^{-1}[P]$或 $b\in\sigma^{-1}[P]$.

17. $f(x)=a_nx^n+\cdots+a_0\to\bar{f}(x)=\bar{a}_nx^n+\cdots+\bar{a}_0$ 是同态映射, 同态核中元素形如: $\sum_{i=0}^{n}a_ix^i$, $a_i\in K$, $n>0$, 其中 K 为 R 到 $\bar{R}$ 的同态核.

18. $f\to\bar{f}$ 是同态, 若 $f(x)$可约, 则 $f(x)=f_1(x)\cdot f_2(x)$, f_1,f_2 次数>0, 首项系数为 1, 则 $\bar{f}=\bar{f}_1\cdot\bar{f}_2$. 矛盾.

19. 若 $a_n+a_{n-1}x+\cdots+a_0x^n=(b_m+\cdots+b_0x^m)(c_k+\cdots+c_0x^k)$, 则 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=(b_mx^m+\cdots+b_0)(c_kx^k+\cdots+c_0)$. 反之亦然.

20. 一方面, $(1+1)(a+b)=a+b+a+b$, 另一方面又等于 $a+a+b+b$, 消去两侧 a,b, 得 $b+a=a+b$.

21. 若(1)成立, 设 u_1 和 u_2 是 u 的互异的右逆元, 则 $u(u_1-u_2)=uu_1-uu_2=1-1=0$, 因而 u 是左零因子, (3)成立. 若(3)成立, 如 u 是可逆元, 如果 $uv=0, v\neq0$, 则 $u^{-1}uv=0$, 因而 $v=0$, 矛盾. 即 u 不是可逆元. 若(2)成立, u 只有一个右逆元 $u_1, uu_1=1$, 但 $u(u_1u-1+u_1)=u-u+1=1$, 故 $u_1u-1+u_1=u_1$, 或 $u_1u=1$, 推出 u 可逆, 矛盾.

22. 设 u 的右逆元集为 A. A 中任取定一个元素 a_0, 设 $B=\{xu-1+a_0|x\in A\}$. 易证 $B\subseteq A$; 由上题, u 的右逆元不是左逆元 (否则 u 可逆), $xu-1\neq0$, $xu-1+a_0\neq a_0$, $(x\in A)$. 故 $a_0\notin B$. 映射 $\sigma(x)=xu-1+a_0(x\in A)$ 易证是 A 到 B 的一一映射, 即 $A\sim B$, A 与真子集 B 等势, 推出 A 为无限集.

习题 5·1

1. p.

2. (1) $(a+b)^{p^n}=(\cdots(a+b)^p\cdots)^p=(\cdots(a^p+b^p)^p\cdots)^p=\cdots=a^{p^n}+b^{p^n}$. (2) 证法同上。 (3) $(a_1+a_2+\cdots+a_n)^p=(a_1+(a_2+\cdots+a_n))^p=a_1^p+(a_2+\cdots+a_n)^p=\cdots=a_1^p+a_2^p+\cdots+a_n^p$. (4) $(n\cdot 1)^p=(1+1+\cdots+1)^p=1^p+1^p+\cdots+1^p=1+1+\cdots+1=n$. (5) $(a-b)^p=(a-b)(a-b)^{p-1}$. 而 $(a-b)^p=a^p-b^p=(a-b)(a^{p-1}+ab^{p-2}+\cdots+a^{p-2}b+b^{p-1})$，设 $a-b\neq 0$，域中无零因子，故$(a-b)^{p-1}=a^{p-1}+ab^{p-2}+\cdots+a^{p-2}b+b^{p-1}$. 若 $a=b$，上式仍成立，因右端化为 $pa^{p-1}=0$。

3. (1) $[5^7]=[5]^7=([2]+[3])^7=[2]^7+[3]^7=[2^7]+[3^7]$。(2) $[5^7]=([1]+\cdots+[1])^7=[1]^7+\cdots+[1]^7=[1]+\cdots+[1]=[5]$。

4. 利用定理 4。

5. 域与子域有公共的零元 0 和单位元 1，故在方程 $n1=0$ 的最小正整数解是共同的。

6. $1\in \mathbf{Q}(i)=\{a+bi\mid a,\ b\in\mathbf{Q}\}\neq\phi$. 设 $a+bi$，$c+di\in\mathbf{Q}(i)$，$(a+bi)-(c+di)=(a+c)-(b+d)i\in\mathbf{Q}(i)$，$(a+bi)\cdot$

$$(c+di)^{-1}=\frac{1}{(c^2+d^2)}[(ac+bd)+(bc-ad)i]\in\mathbf{Q}(i).$$

7. $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\to a+bi$ 是同构映射。

8. $1=1^p\in F^p\neq\phi$. 任取 a^p，$b^p\in F^p$，则 $a^p-b^p=(a-b)^p\in F^p$. $a^p\cdot(b^p)^{-1}=(ab^{-1})^p\in F^p(b\neq 0)$。

9. $(a+b)^p=a^p+b^p$. $(a\cdot b)^p=a^p\cdot b^p$。

10. 由上题，只须证明是一一映射．若 $a\neq b$，则$(a-b)^p=a^p-b^p$，故 $a^p\neq b^p$. $a\to a^p$ 是单射，由于F元素有限，故

也是一一映射（习题1·2—9）。

11. $F_1\neq\phi$. 任取 ab^{-1}, $cd^{-1}\in F_1$, 则 $ab^{-1}-cd^{-1}=(ad-bc)(bd)^{-1}\in F_1$. $(ab^{-1})(cd^{-1})^{-1}=(ad)(bc)^{-1}\in F_1$（设 $cd^{-1}\neq 0$）。F_1是F子域. 设E是包含R的任一子域，则显然包含 ab^{-1}(a, $b\in R$, $b\neq 0$)，故包含 F_1。

习题 5·2

1. $\mathbf{Q}(i)$ 是$\mathbf{Z}[i]$的扩域. 任取$\frac{b}{a}+\frac{d}{c}i\in\mathbf{Q}(i)$, ($a,b,c,d\in\mathbf{Z}$, $a,c\neq 0$)则它等于$(bc+adi)(ac+0i)^{-1}$。

2. $\mathbf{Q}$是$\mathbf{E}$的扩域，任取$\frac{b}{a}\in\mathbf{Q}$, 则$\frac{b}{a}=(2b)(2a)^{-1}$。

4. R 的分式域是 $\mathbf{Q}$。

习题 5·3

1. (1) x^2-2x-1; (2) $x^4-10x+1$; (3) x^2-2x+2; (4) $x^6-3x^4+3x^2-3$。

2. (1) $a_0+a_1\alpha$; (2) $a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3$; (3)$a_0+a_1\alpha$; (4) $a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4+a_5\alpha^5$。

3. $[1]x^3-[1]x-[1]=f(x)$. $\mathbf{Z}_3[x]/\langle f(x)\rangle$含 27 个元素的域。

4. (1)(2)(4)(5)(6)。

5. β形如$\frac{f(\alpha)}{g(\alpha)}$, f、g是互素的多项式. 若β是代数元，设为$h(x)=a_nx^n+\cdots+a_0$的根， 则$a_n\left(\frac{f(\alpha)}{g(\alpha)}\right)^n+\cdots+a_0=0$，因而$a_n(f(\alpha))^n+\cdots+a_0(g(\alpha))^n=0$. 设$k(x)=a_n(f(x))^n+a_{n-1}(f(x))^{n-1}g(x)+\cdots+a_0(g(x))^n$，$g(x)$ 整除上式的除第

一项外的其他项，因而 $g(x)\nmid k(x)$，$k(x)\neq 0(x), k(\alpha)=0$，与 α 是超越元矛盾。所以 β 是超越元。

6. $p(x)$是三次多项式，若可约必有根，但 $p([1])=[1]=p([0])$，故 $p(x)$既约。在同构的意义下，$\mathbf{Z}_2[x]/\langle p(x)\rangle$ 包含 $p(x)$ 的根。

7. 在 $E(\alpha)[x]$中，$(x-\alpha)\mid p(x),(x-\alpha)\mid q(x)$，故 $p(x)$ 与 $q(x)$不互素，在 $E[x]$中 $p(x)$与 $q(x)$仍不互素。由于 $q(x)$ 既约，必有 $q(x)\mid p(x)$。

8. (1) $\mathbf{Q}(\sqrt[3]{2})$ 的元素形如 $a+b\sqrt[3]{2}+c\sqrt[3]{4}$。用待定系数法求逆元。由$(1+\sqrt[3]{2})(a+b\sqrt[3]{2}+c\sqrt[3]{4})=1$，得 $(a+2c)+(a+b)\sqrt[3]{2}+(b+c)\sqrt[3]{4}=1$，解出 $a=c=\frac{1}{3}$，$b=-\frac{1}{3}$，即$(1+\sqrt[3]{2})^{-1}=\frac{1}{3}(1-\sqrt[3]{2}+\sqrt[3]{4})$。(2) ε 是二次元，同法可求得 $(5+6\varepsilon)^{-1}=-\frac{1}{31}-\frac{6}{31}\varepsilon$。 (3) $[2]\alpha^2+[2]\alpha+[1]$。(4) $\frac{1}{6}(\sqrt[3]{25}-\sqrt[3]{5}+1)$。

9. 和：$8x-2+\langle x^2-2\rangle$，积：$2x+6+\langle x^2-2\rangle$。

习题 5·4

1. 2；2；8。基：$1,\sqrt{2}$；$1,\sqrt{3}$； $1,\sqrt{2},\sqrt{3},\sqrt{6},\sqrt{5},\sqrt{10},\sqrt{15},\sqrt{30}$。

2. 只须证明 x^2-2 在 $\mathbf{Q}(\sqrt[3]{2})$上无根。假若 $a+b\sqrt[3]{2}+c\sqrt[3]{4}$是根，$(a+b\sqrt[3]{2}+c\sqrt[3]{4})^2=2$，即 $(a^2+4bc)+(b^2+2ac)\sqrt[3]{4}+(2c^2+2ab)\sqrt[3]{2}=2$。$a^2+4bc=2$，$b^2+2ac=0$，$2c^2+2ab=0$。$a^2b^2=c^4$，$-a^2(2ac)=c^4$，$c(2a^3+c^3)=0$，$c$

$\neq 0$,否则,$a^2=2$不可能。故 $2a^3+c^3=0$,$2=-\frac{c^3}{a^3}=-\left(\frac{c}{a}\right)^3$ 不可能。

3. 令 $\alpha=\sqrt{2}+\sqrt{3}$,则$(\sqrt{2}-\alpha)^2=3$, 即 $2+\alpha^2-2\alpha\sqrt{2}=3$,$\sqrt{2}=\frac{1-\alpha^2}{-2\alpha}\in\mathbf{Q}(\alpha)$,同理$\sqrt{3}\in\mathbf{Q}(\alpha)$,因而 $\mathbf{Q}(\sqrt{2},\sqrt{3})\subseteq\mathbf{Q}(\alpha)$。但 $\alpha=\sqrt{2}+\sqrt{3}\in\mathbf{Q}(\sqrt{2},\sqrt{3})$,故 $\mathbf{Q}(\sqrt{2}+\sqrt{3})\subseteq\mathbf{Q}(\sqrt{2},\sqrt{3})$。

4. 由于$[K:F]=[K:E][E:F]=[K:E]$,故$[E:F]=1$。

5. 任取 $\alpha\in E\backslash F$,则 $p=[E:F]=[E:F(\alpha)][F(\alpha):F]$。而$[F(\alpha):F]\neq 1$,是 p 的因子,必是 p,而$[E:F(\alpha)]=1$,$E=F(\alpha)$。

6. 假若 $p(x)$ 在 E 中有根 α,则 $\alpha\bar{\in}F$。显然 $F\subseteq F(\alpha)\subseteq E$。故$[E:F]=[E:F(\alpha)][F(\alpha):F]$,$[F(\alpha),F]=p(x)$的次数$>1$,整除$[E:F]$,与已知互素条件矛盾。

7. $F[x]$是主理想环 $E[x]$的子环,利用习题 4·6—9。

习题 5·5

1. 若 $f(x)$可约,必形如 $f(x)=(x-\alpha)(x-\beta)$,因而 F 是 $f(x)$的分裂域;若 $f(x)$既约,作单代数扩域 $F(\alpha)$,使其包含 $f(x)$的根 α。$F(\alpha)[x]$中 $f(x)=(x-\alpha)g(x)$,$g(x)$应形如 $x-\beta$,即 $f(x)=(x-\alpha)(x-\beta)$,$F(\alpha)$是 $f(x)$的分裂域。

2. 6 次扩域。令 $u=\sqrt[3]{5}$(实数),$x-u$ 在 $\mathbf{Q}(u)[x]$ 中整除 x^3-5。经计算可知 $x^3-5=(x-u)(x^2+ux+u^2)$。x^2+ux+u^2 的根是 $v=\frac{-1+\sqrt{3}i}{2}u$,$w=\frac{-1-\sqrt{3}i}{2}u$。它们不是

实数，故不在 $\mathbf{Q}(u)$ 中，因而 x^2+ux+u^2 在 $\mathbf{Q}(u)$ 上既约。$v+w=-u, v=-u-w, w=-v-u$，故 $\mathbf{Q}(u)(v)=\mathbf{Q}(u)(w)=L$ 是 x^3-2 的分裂域。$[L:\mathbf{Q}]=[L:\mathbf{Q}(u)][\mathbf{Q}(u):\mathbf{Q}]=2\cdot3=6$。

3．对多项式的次数使用归纳法。当 $n=1$ 时显然成立。设对于次数 $<n$ 时成立，假定 $f(x)$ 是 n 次多项式。如果 $f(x)$ 可约，$f(x)=f_1(x)f_2(x)$，$f_1(x), f_2(x)$ 的次数分别是 n_1, n_2，$f_1(x)$ 的分裂域 E 关于 F 扩域的次数依照归纳假定至多为 $n_1!$，而 $f_2(x)$ 的分裂域 K 关于 E 扩域的次数依照归纳假定至多为 $n_2!$。因而 $f(x)$ 的分裂域关于 F 扩域的次数至多为 $n_1!\cdot n_2!<n!$。如果 $f(x)$ 既约，作单扩域 $F(\alpha)$ 使其包含 $f(x)$ 的根 α，$[F(\alpha):F]=n$，在 $F(\alpha)$ 上 $f(x)=(x-\alpha)g(x)$，$g(x)$ 次数 $=n-1$，依照归纳假定 $g(x)$ 分裂域关于 $F(\alpha)$ 扩域次数至多为 $(n-1)!$ 因而 $f(x)$ 分裂域关于 F 扩域的次数至多为 $n\cdot(n-1)!=n!$。

4．x^n-1 的根为 $\theta^0, \theta, \theta^2, \cdots, \theta^{n-1}$，显然属于 $\mathbf{Q}(\theta)$。

5．$f(x)=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$，$x^{p-1}+\cdots+1$ 是 $\mathbf{Q}$ 上的既约多项式（见《多项式代数》），其分裂域 $E=\mathbf{Q}(\theta)$，θ 为 p 次原根，是 $x^{p-1}+\cdots+1$ 的根，$F(\theta)$ 为 $p-1$ 扩域。

6．4．x^2-2 是 $\mathbf{Q}$ 上的既约多项式，设 $\mathbf{Q}(\alpha)$ 是 $\mathbf{Q}$ 的单扩域，α 是 x^2-2 的根。$\mathbf{Q}(\alpha)$ 元素形如 $a+b\alpha$。x^2-3 在 $\mathbf{Q}(\alpha)$ 上既约，否则必有根，设根为 $a+b\alpha$，则 $(a+b\alpha)^2=3$。$a^2+2b^2+2ab\alpha=3, ab=0, a^2+2b^2=3$。若 $b=0$。得 $a^2=3$，不可能。若 $a=0$，则 $b^2=\dfrac{3}{2}$，不可能。作单扩域 $\mathbf{Q}(\alpha)(\beta)$，其中 β 是 x^2-3 的根。所以，得到 $f(x)$ 的分裂域 $[\mathbf{Q}(\alpha)(\beta):\mathbf{Q}(\alpha)][\mathbf{Q}(\alpha):\mathbf{Q}]=2\cdot2=4$。

习题 5·6

1. (1)、(2)、(5)无重根，(3)、(4)有重根.

2. 若 $x^{p^n}-a$ 既约，但 $a=b^p$，则 $x^{p^n}-b^p=(x^{p^{n-1}}-b)^p$ 可约. 反之，若 a 不是任意元素的 p 次幂，则类似于定理3证明的前半部可证得结论.

3. 设 E 是 F 的代数扩域，K 是 E 的不可分扩域，$\alpha\in K$ 是 E 的不可分元素，则有 E 上的不可分既约多项式 $p(x)$ 以 α 为根. 但 K 也是 F 的扩域，故是可分扩域，α 是 F 上的可分元素，设其极小多项式为 $q(x)$，$q(x)$ 无重根. 在 $E[x]$ 中 $p(x)|q(x)$. $q(x)$ 无重根，故 $p(x)$ 也无重根，矛盾.

4. $\alpha_1=\sqrt{2}\,i$，$\alpha_2=\dfrac{-1+\sqrt{3}\,i}{2}$，$\beta_2=-\sqrt{2}\,i$，$\gamma_2=\dfrac{-1-\sqrt{3}\,i}{2}$，取 $c\neq\dfrac{\beta_2-\alpha_1}{\alpha_2-\gamma_2}$，$c\neq 0$. 如取 $c=1$，$\alpha=\alpha_1+\alpha_2=\dfrac{-1+(2\sqrt{2}+\sqrt{3})i}{2}$.

5. x^2+x+1 的根为 $\dfrac{-1+\sqrt{3}\,i}{2}$，$\dfrac{-1-\sqrt{3}\,i}{2}$；$x^2+4$ 的根为 $2i,-2i$. 取 $c\neq\pm\dfrac{\frac{1}{2}(-1+\sqrt{3}\,i)-\frac{1}{2}(-1-\sqrt{3}\,i)}{4i}$ 且 $c\neq 0$，如取 $c=1$，$t=\dfrac{-1+\sqrt{3}\,i}{2}+2i$.

7. 由(2)式知 D 为同态. 核为全体零次及零多项式的集合，即为 F.

习题 5·7

1. $x^{125}-x$ 在 $\mathbf{Z}_5$ 上的分裂域。

2. 这时商环是整环，且是有限集，故为域。

3. $|F^*|=32-1=31$ 是素数，与之互素的较 31 小的数有 30 个，故有 30 个本原元。

4. 由定理 7，p^q 元域的子域为 p^m 元域，$m|q$，只能 $m=1$ 或 q，故只有平凡子域。

5. $\alpha^4+\alpha$。

6. $2\alpha^2+2\alpha+1$。

复习题五

1. $F(\alpha)$ 中 α^{-1} 设为 $b_0+b_1\alpha+b_2\alpha^2+\cdots+b_{n-2}\alpha^{n-2}+b_{n-1}\alpha^{n-1}$。利用 $\alpha\alpha^{-1}=1$ 和 $\alpha^n=-a_0-a_1\alpha-\cdots-a_{n-1}\alpha^{n-1}$ 待定系数求出 $-a_0b_{n-1}=1$，$b_0-b_{n-1}a_1=0$，$b_1-b_{n-1}a_2=0$，…，$b_{n-2}-b_{n-1}a_{n-1}=0$，得 $b_{n-1}=-a_0^{-1}$，$b_0=-a_1a_0^{-1}$，$b_1=-a_2a_0^{-1},\cdots,b_{n-2}=-a_{n-1}a_0^{-1}$。

2. $2a=0$，$a=-a$。

3. K 在 F 上的基设为 $\{1,u\}$，则 $K=\{au+b\,|\,a,b\in F\}$。K 包含 u^2，设为 $au+b$。故 $\left(u-\dfrac{a}{2}\right)^2=b+\dfrac{a^2}{4}$，令 $v=u-\dfrac{a}{2}$，则 (1，v) 也是基，且 $K=F(v)$，其中 $v^2=b+\dfrac{a^2}{4}=w\in F$。故 $K=F(\sqrt{w})$。

4. 设 $[F:\mathbf{R}]=n$。若 $n=1$，则 $F\cong\mathbf{R}$。否则，$n>1$，且有 $\alpha\in F\setminus\mathbf{R}$。$\{1,\alpha,\alpha^2,\cdots,\alpha^n\}$ 线性相关（元数 $>n$），故有

$\lambda_0,\lambda_1,\cdots,\lambda_n\in \boldsymbol{R}$，不全为零，使 $\lambda_0+\lambda_1\alpha+\cdots+\lambda_n\alpha^n=0$，即 α 是 $\boldsymbol{R}$ 上的代数元，但因 $\boldsymbol{R}$ 上的既约多项式只有一次及二次多项式。α 必满足 $\boldsymbol{R}$ 上的一次或二次方程.若满足一次方程，则 $\alpha\in\boldsymbol{R}$，与假定矛盾，否则 $[\boldsymbol{R}(\alpha):\boldsymbol{R}]=2$。由上题，$\boldsymbol{R}(\alpha)=\boldsymbol{R}(\sqrt{\beta})$，$\beta$ 是负数(因为 $\boldsymbol{R}$ 包含所有正数平方根)，因而 $\sqrt{\beta}=ir$，$r\in\boldsymbol{R}$，$\boldsymbol{R}(\alpha)=\boldsymbol{R}(i)=\boldsymbol{C}$。故 F 有子域同构 $\boldsymbol{C}$，且 $[F:\boldsymbol{C}]=[F:\boldsymbol{R}]/2$.它是有限扩域.类似上面讨论，知 F 中任意元素是 $\boldsymbol{C}$ 上既约多项式的根．但 $\boldsymbol{C}$ 上唯有一次式既约，其根在 $\boldsymbol{C}$ 中，因而 $F\cong\boldsymbol{C}$。

5．设 $g(x)\in F[x]$ 是 $x^{p^n}-\gamma$ 的真因子。在 F 的某一扩域上，$x^{p^n}-\gamma=x^{p^n}-\alpha^{p^n}=(x-\alpha)^{p^n}$。故 $g(x)$ 形如 $(x-\alpha)^{pj}$，$1\leqslant j\leqslant n-1$，故 $\alpha^{pj}\in F$，$\alpha^{p^{n-1}}=(\alpha^{pj})^{p^{n-j-1}}\in F$，矛盾。

6．设 E 是完全域 F 的代数扩域．假若 E 上既约多项式 $p(x)$ 在其分裂域 K 中有重根 α，即在 $K[x]$ 中 $(x-\alpha)^2|p(x)$。K 是 E 的因而是 F 的代数扩域，α 是 F 上的代数元，设 α 在 F 上的极小多项式为 $q(x)$，则在 $K[x]$ 中 $x-\alpha|q(x)$，$q(x)$ 与 $p(x)$ 在 $K[x]$ 中不互素，在 $E[x]$ 中也不互素(习题5·4—7)，而 $p(x)$ 是 $E[x]$ 中既约多项式，故 $p(x)|q(x)$，推得 $q(x)$ 也有重根 α，与 F 是完全域矛盾．所以 E 是完全域。

7．不是．假若 σ 是 $\boldsymbol{Q}(\sqrt{2})$ 到 $\boldsymbol{Q}(\sqrt{3})$ 的等价同构映射，$\sigma(a)=a$ 对一切 $a\in\boldsymbol{Q}$ 成立。设 $\sigma(\sqrt{2})=a+b\sqrt{3}$。$\sigma(\sqrt{2})^2=\sigma(2)=2$，即 $(a+b\sqrt{3})^2=a^2+3b^2+2\sqrt{3}\,ab=2$。$a^2+3b^2=2$，$ab=0$。如果 $b=0$，$a^2=2$，不可能；如果 $a=0$，$b^2=\frac{2}{3}$，不可能．σ 不存在．同理可证 $\boldsymbol{Q}(\sqrt{2})$ 与

$\mathbf{Q}(i)$也不等价等。

8. 在$F(\alpha)$中，$a^p-a=0$，$a=\alpha^p$。因而多项式在$F(\alpha)$上化为$x^p-a=x^p-\alpha^p=(x-\alpha)^p$，可以分解为一次因子之积。

9. 由§5·3定理7，存在F的单扩域$F(\alpha_1)$包含$p(x)$的根α_1，若$q(x)$已在$F(\alpha_1)[x]$中完全分解为一次因子之积，任取其根作为α_2即可。若$q(x)$不能在$F(\alpha_1)$上分解为一次因子之积，则有既约因子$q_1(x)$，再作单扩域$F(\alpha_1)(\alpha_2)$使α_2是$q_1(x)$的根，$F(\alpha_1, \alpha_2)=F(\alpha_1)(\alpha_2)$即为所求。

10. 否则必有根，设为$a+b\sqrt{3}$。$(a+b\sqrt{3})^3=2$。$(a^3+9ab^2)+(3a^2b+9b^3)\sqrt{3}=2$。$a^3+9a^2b=2$，$3a^2b+9b^3=0$。$b(a^2+3b^2)=0$。若$b=0$，则$a^3=2$，不可能；若$a^2+3b^2=0$，则$a=b=0$，$0=2$，不可能。

11. 设K是$f(x)$在E上的分裂域，$\alpha\in K$是$f(x)$的根，则由于K是E的因而是F的代数扩域，α是F的代数元，故α在F上有极小多项式，设为$q(x)$，在$K[x]$中$f(x)$与$q(x)$有公因式$x-\alpha$，因而不互素，在$E[x]$中也不互素(习题5·4—9)，由$f(x)$的既约性，$f(x)|q(x)$。

12. 在$\mathbf{Q}(\alpha)$上，$x^3-a=(x-\alpha)(x^2+\alpha x+\alpha^2)$，另外两根是$x^2+\alpha x+\alpha^2$的根$\alpha\varepsilon$和$\alpha\varepsilon^2$($\varepsilon$为三次原根)。若$\mathbf{Q}(\alpha)$是$x^3-a$的分裂域，则$\alpha\varepsilon$，$\alpha\varepsilon^2\in F(\alpha)$、于是，$F\subseteq F(\varepsilon)\subseteq F(\alpha)$。$[F(\varepsilon):F]\,|\,[F(\alpha):F]$，即2整除3，矛盾($\varepsilon$的极小多项式为$x^2+x+1$)。

13. $[E(\alpha):F(\alpha)][F(\alpha):F]=[E(\alpha):F]=[E(\alpha):E][E:F]$，$[F(\alpha):F]\,|\,[E(\alpha):E]$(因$[F(\alpha):F]$与$[E:F]$互素)。但由于$\alpha$在$E$上的极小多项式整除$\alpha$在$F$上的极小多项式，

故$[E(a):E]\leqslant[F(a):F]$. 因而$[E(a):E]=[F(a):F]$.

习题 6·1

1. 一次代数.

2. 包括 4 个元素：$a_1=[0]a+[0]e$, $a_2=[0]a+[1]e$, $a_3=[1]a+[0]e$, $a_4=[1]a+[1]e$. 其运算如下：(1) $[0]a_i=a_1$, $[1]a_i=a_i$, $i=1, 2, 3, 4$. (2) 加法与乘法如表所示：

+	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_1	a_4	a_3
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_3	a_2	a_1

·	a_1	a_2	a_3	a_4
a_1	a_1	a_1	a_1	a_1
a_2	a_1	a_2	a_3	a_4
a_3	a_1	a_3	a_2	a_4
a_4	a_1	a_4	a_4	a_1

4. $a(kb+lc)=a(kb)+a(lc)=k(ab)+l(ac)$;
$(kb+lc)a=(kb)a+(lc)a=k(ba)+l(ca)$.

5. G关于·适合结合律：$(x\cdot y)\cdot z=y\cdot z=z=x\cdot(y\cdot z)$. 故此群胚代数为半群代数.

习题 6·2

1. 设$G=\{a_1, a_2,\cdots,a_m,\cdots,a_n\}$, $H=\{a_1,\cdots,a_m\}$. H在F的群代数元素形如$k_1a_1+\cdots+k_ma_m$. 改写为$k_1a_1+\cdots+k_ma_m+0a_{m+1}+\cdots+0a_n$ (0 是F的零元), 成为G在F上群代数的元素. 上形元素关于G在F上群代数的运算显然是封闭的, 故作成子代数.

2. $\{0\}$, $\boldsymbol{C}$, $\boldsymbol{R}$.

4. I_x 是理想，且任意包含 x 的理想也包含 I_x 中的所有元素。

5. $[(a+I)\cdot(b+I)]\cdot(c+I)=(ab+I)\cdot(c+I)$
$=(ab)c+I=a(bc)+I=(a+I)\cdot[(b+I)\cdot(c+I)]$

6. 类似于§4·4 中各定理的证明。

7. 任取 $\alpha=a_1a+a_2b+a_3c+a_4d\in \boldsymbol{R}(B_4)$，则

$$\begin{cases} a\alpha=a_1a+a_2b+a_3c+a_4d,\\ b\alpha=a_1b+a_2a+a_3d+a_4c,\\ c\alpha=a_1c+a_2d+a_3a+a_4b,\\ d\alpha=a_1d+a_2c+a_3b+a_4a. \end{cases}$$

因而

$$\varphi(\alpha)=\begin{pmatrix} a_1 & a_2 & a_3 & a_4\\ a_2 & a_1 & a_4 & a_3\\ a_3 & a_4 & a_1 & a_2\\ a_4 & a_3 & a_2 & a_1 \end{pmatrix}.$$

是 $\boldsymbol{R}(B_4)$在 $M_4(\boldsymbol{R})$中的正则表示。

习题 6·3

1. $N(\alpha\beta)=(\alpha\beta)\overline{\alpha\beta}=\alpha\beta\bar{\beta}\bar{\alpha}=\alpha(\beta\bar{\beta})\bar{\alpha}=(\beta\bar{\beta})(\alpha\bar{\alpha})=N(\alpha)N(\beta)$.（$\beta\bar{\beta}$ 是实数，故可与 α 交换）。

2. 任取 $\alpha=a+bi+cj+dk\in \boldsymbol{H}$，则 $1\alpha=a+bi+cj+dk$，$i\alpha=ia-b+ck-dj$，$j\alpha=aj-bk-c+di$，$k\alpha=ak+bj-ci-d$。

$$\varphi(\alpha)=\begin{pmatrix} a & b & c & d\\ -b & a & -d & c\\ -c & d & a & -b\\ -d & -c & b & a \end{pmatrix}$$

是 $\boldsymbol{H}$ 到 $M_4(\boldsymbol{R})$ 中的正则表示。

3．设 $(1+i-j+k)^{-1}=a+bi+cj+dk$，则 $(1+i-j+k)(a+bi+cj+dk)=(a-b+c-d)+(a+b-c-d)i+(-a+b+c-d)j+(a+b+c+d)k=1$。对比得四元方程组，解得：$a=c=\frac{1}{4}$，$b=d=-\frac{1}{4}$。所以 $(1+i-j+k)^{-1}=\frac{1}{4}-\frac{1}{4}i+\frac{1}{4}j-\frac{1}{4}k$。

4．任意实数显然与四元数可换，另一方面，若 x 属于中心，$x=a+bi+cj+dk$，则 $xi=ai-b-ck+dj$，$ix=ai-b+ck-dj$，由 $xi=ix$ 得 $c=d=0$。再由 $xj=jx$ 或 $xk=kx$ 可得 $b=0$，$x=a\in\boldsymbol{R}$。

5．设 $\alpha=a_1+b_1i+c_1j+d_1k$，$\beta=a_2+b_2i+c_2j+d_2k$，则 $\overline{\alpha+\beta}=\overline{(a_1+a_2)+(b_1+b_2)i+(c_1+c_2)j+(d_1+d_2)k}=(a_1+a_2)-(b_1+b_2)i-(c_1+c_2)j-(d_1+d_2)k=(a_1-b_1i-c_1j-d_1k)+(a_2-b_2i-c_2j-d_2k)=\bar{\alpha}+\bar{\beta}$。$\overline{\alpha\beta}=\bar{\beta}\bar{\alpha}$ 可通过展开整理验证。$\alpha\bar{\alpha}=(a_1^2+b_1^2+c_1^2+d_1^2)+0i+0j+0k=a_1^2+b_1^2+c_1^2+d_1^2$，同样可证 $\bar{\alpha}\alpha=a_1^2+b_1^2+c_1^2+d_1^2$。

6．设 $x=a+bi+cj+dk$，则 $(1+j)(a+bi+cj+dk)=2+i-k$。展开整理，对比得方程组 $2=a-c$，$1=b+d$，$0=c+a$，$-1=d-b$。解得 $a=1$，$b=1$，$c=-1$，$d=0$。

7．$(q^{-1}\alpha q)^2+a_0(q^{-1}\alpha q)+b_0=q^{-1}\alpha^2q+q^{-1}(a_0\alpha)q+q^{-1}b_0q=q^{-1}(\alpha^2+a_0\alpha+b_0)q=q^{-1}0q=0$。

复习题六

1．设代数的基为 $\{1,\beta\}$，任意元素形如：$a_1+a_2\beta$ $(a_1,$

$a_2\in F$)。显然 $(a_1+a_2\beta)(b_1+b_2\beta)=a_1b_1+a_1b_2\beta+a_2b_1\beta+a_2b_2\beta^2=(b_1+b_2\beta)(a_1+a_2\beta)$。

2．不是。$\boldsymbol{C}$ 是 $\boldsymbol{R}$ 上的二次代数，而 $\boldsymbol{R}(G)$ 是 $\boldsymbol{R}$ 上的四次代数。

3．设 $c\in C$，$a\in A$，σ 为 A 的任一自同构，$\sigma^{-1}(a)=a_1$，$\sigma(a)=a_2$，由于 $ca_1=a_1c$，$\sigma(c)\sigma(a_1)=\sigma(a_1)\sigma(c)$，即 $\sigma(c)a=a\sigma(c)$，$\sigma(c)\in C$。由于 $ca_2=a_2c$，σ^{-1} 也是自同构，$\sigma^{-1}(c)\sigma^{-1}(a_2)=\sigma^{-1}(a_2)\sigma^{-1}(c)$，或 $\sigma^{-1}(c)a=a\sigma^{-1}(c)$。$\sigma^{-1}(c)\in C$。$\sigma[C]=C$。

5．子空间关于乘法封闭（积总是零）。

6．作 $F[x]$ 到 F 的映射：$f(x)\to f(0)$。易证这是代数同态，核为 $F_0[x]$。由 § 6·2 定理 2 得证。

7．子群：G，$\{1\}$，$\{1,-1\}$，$\{1,-1,i,-i\}$，$\{1,-1,j,-j\}$，$\{1,-1,k,-k\}$。G 不是可换群（如 $ij=k\neq-k=ji$），故不与 C_8 同构。G 只有一个 2 阶元 -1，但 D_4 有五个 2 阶元：R_π，V，H，D_1，D_2。故 G 也不与 D_4 同构。

8．参见习题 4·3—6。另外，注意 $(ka)^n=k^na^n=0$（$k\in F$）。

9．设 $(ab)^n=0$，$(ba)^{n+1}=baba\cdots ba=b(ab)^na=0$。

10．令 $F_1=\{ke\mid k\in F\}\subseteq A$，$\varphi(k)=ke$。显然 $\varphi(k+l)=(k+l)e=ke+le=\varphi(k)+\varphi(l)$，$\varphi(kl)=(kl)(ee)=k(l(ee))=k(e(le))=(ke)(le)=\varphi(k)\varphi(l)$，因而 φ 是 F 到 F_1 的同态，且是满射。$\varphi(1)=1e=e\neq0$，故 φ 为同构。$F\cong F_1$，F_1 为域。任取 $a\in A$，则 $(ke)a=k(ea)=k(ae)=a(ke)$，$F_1\subseteq$ 中心。

11．只须证明方程 $ax=b$，$ya=b$ 都有唯一解（$a\neq0$）。aR

$=\{ar \mid r\in R\}$显然是R的子空间．若$aR\neq R$，设$x_1,\cdots,x_n$是R的基，则$ax_1,\cdots,ax_n$必线性相关，即存在F中不全为零的数$k_1,\cdots,k_n$，使$k_1(ax_1)+\cdots+k_n(ax_n)=0$，或

$$a(k_1x_1+\cdots+k_nx_n)=0$$

以上两因子都$\neq 0$，R又无零因子，推出矛盾，所以$aR=R$。由于R无零因子，故解是唯一的．同理可知方程$ya=b$也有唯一解。

12．参考§6·3引理2的证明。

13．$\alpha^2=(a_0+a_1i+a_2j+a_3k)^2=a_0^2-a_1^2-a_2^2-a_3^2+2a_0a_1i+2a_0a_2j+2a_0a_3k$, $T(\alpha)\alpha=2a_0^2+2a_0a_1i+2a_0a_2j+2a_0a_3k$, $N(\alpha)=a_0^2+a_1^2+a_2^2+a_3^2$。

所以　$\alpha^2-T(\alpha)\alpha+N(\alpha)=0$。

习题 7·1

1．n元集的任一排列可以构成一种全序关系，故共有$n!$种全序关系。

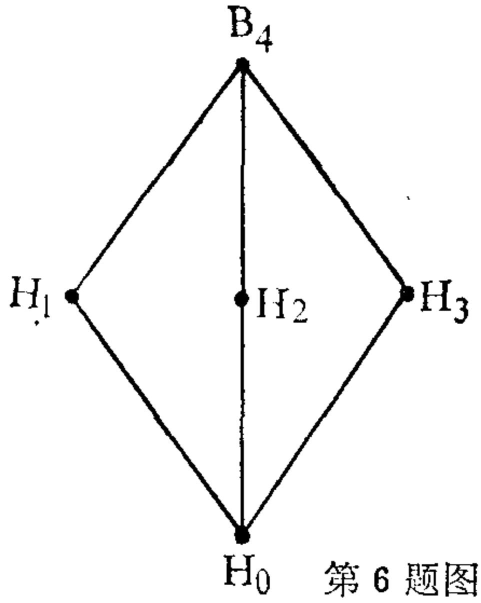
2．(1)(2)不是半序集，不适合反对称性；(3)是半序集，不是全序集；(4)是全序集；(5)关于整除关系作成半序集，而关于大小作成全序集。

3．(4)单位元是整个群，零元是单位元子群$\{e\}$；(5)关于整除关系的零元是1，关于大小的单位元是5，零元是1。

4．由于$a_2\leqslant a_3\leqslant\cdots\leqslant a_n\leqslant a_1$，故$a_2\leqslant a_1$，又因$a_1\leqslant a_2$，故$a_1=a_2$，同理$a_1=a_2=\cdots=a_n$。

5．极大元：g，i；极小元：a，b，c，d；四个确界分别是f，g，e，c。

6. $B_4=\{a, b, c, d\}$ (§3·1例4)的子群有5个：$H_0=\{a\}$，B_4，$H_1=\{a, b\}$，$H_2=\{a, c\}$，$H_3=\{a,d\}$。其覆盖图如右。



第6题图

7. 是。适合半序集的三个条件。

习题7·2

1. (1) 若 $a\leqslant b$，$a\leqslant c$，则 a 是 $\{b, c\}$ 下界，故 $a\leqslant b\wedge c$。反之，若 $a\leqslant b\wedge c$，则$a\leqslant b\wedge c\leqslant b$，$a\leqslant b\wedge c\leqslant c$。(2) 类似(1)。(3) $a\leqslant b\leqslant b\vee d$，$c\leqslant d\leqslant b\vee d$，故 $b\vee d$ 是$\{a,c\}$的上界，$a\vee c\leqslant b\vee d$。同理 $a\wedge c\leqslant b\wedge d$。(4) $d\wedge b\leqslant d\wedge c=a$，但 $a=(d\wedge c)\wedge a=d\wedge(c\wedge a)=d\wedge a\leqslant d\wedge b$，故 $d\wedge b=a$，(5) $c=d\vee a\leqslant d\vee b$，但 $d\vee b\leqslant d\vee c=d\vee(d\vee a)=(d\vee d)\vee a=d\vee a=c$，故 $d\vee b=c$。(6) $c\leqslant a\vee c$，$a\wedge(b\wedge c)=(a\wedge b)\wedge c\leqslant(a\wedge b)\wedge(a\vee c)$。(7) $a\wedge b\leqslant a, a\wedge b\leqslant b\leqslant b\vee c$，$a\wedge c\leqslant a$，$a\wedge c\leqslant c\leqslant b\vee c$，故$(a\wedge b)\vee(a\wedge c)\leqslant a\wedge(b\vee c)$。(8) 由(7)，$(a\wedge b)\vee(a\wedge c)\leqslant a\wedge(b\vee c)$，$(b\wedge a)\vee(b\wedge c)\leqslant b\wedge(a\vee c)$，原左端$\leqslant[a\wedge(b\vee c)]\wedge[b\wedge(a\vee c)]=[a\wedge(a\vee c)]\wedge[b\wedge(b\vee c)]=a\wedge b$。另一方面，显然 $a\wedge b\leqslant(a\wedge b)\vee(a\wedge c)$，$a\wedge b\leqslant(a\wedge b)\vee(b\wedge c)$，故 $a\wedge b\leqslant$原左端。等式成立。

2. 逐字重述定理4的证明，只是将"上确界"改为"下确界"，"单位元"改为"零元"。

3. 不能。因无单位元。可用下法证明：设 b 为单位元，

$b<1$，取 $b_1=\frac{1}{2}(b+1)$，则 $b<b_1<1$，b_1 为有理数，与 b 是单位元矛盾。

4. 不能。无单位元。

5. $a\leqslant a\vee b$，$a\leqslant a$，所以 $a\leqslant a\wedge(a\vee b)$，另一方面，显然 $a\wedge(a\vee b)\leqslant a$。

6. 单位元的同态象是单位元，零元的同态象是零元，可由格同态的保序性推出。

7. $\{H_0, H_1, H_2, B_4\}$，$\{H_0, H_1, H_3, B_4\}$，$\{H_0, H_2, H_3, B_4\}$。见习题 7·1—6。

8. 由(L_4)，$a=a\vee(a\wedge(a\vee b))=a\vee a$，$a=a\wedge(a\vee(a\wedge b))=a\wedge a$。

习题 7·3

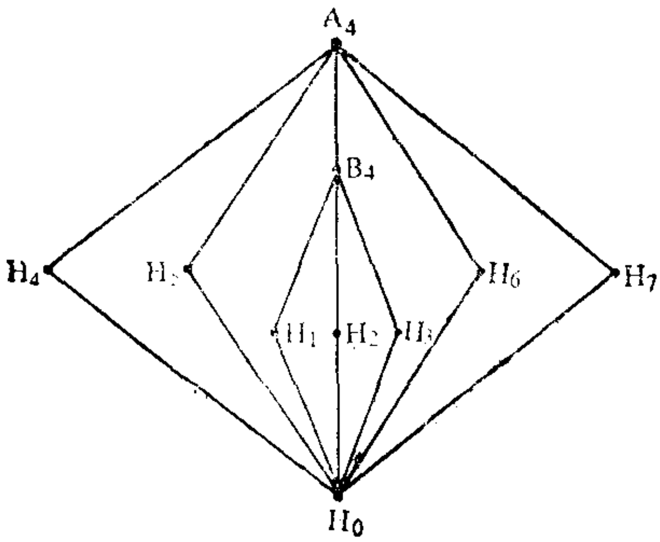
1. $(a+bi)\wedge[(a_1+b_1i)\vee(a_2+b_2i)]=(a+bi)\wedge[\max\{a_1,a_2\}+i\max\{b_1,b_2\}]=\min\{a,\max\{a_1,a_2\}\}+i\min\{b,\max\{b_1,b_2\}\}$。而$[(a+bi)\wedge(a_1+b_1i)]\vee[(a+bi)\wedge(a_2+b_2i)]=\max\{\min\{a,a_1\},\min\{a,a_2\}\}+i\max\{\min\{b,b_1\},\min\{b,b_2\}\}$。易证它们相等。同理可证另一等式。

2. $\varphi(x\vee y)=(x\vee y)\wedge a=(x\wedge a)\vee(y\wedge a)=\varphi(x)\vee\varphi(y)$，$\varphi(x\wedge y)=(x\wedge y)\wedge a=(x\wedge y)\wedge(a\wedge a)=(x\wedge a)\wedge(y\wedge a)=\varphi(x)\wedge\varphi(y)$，$\varphi$ 是格自同态。任取 $\varphi(x),\varphi(y)\in\varphi[L]$，$\varphi(x)\vee\varphi(y)=\varphi(x\vee y)\in\varphi[L]$，$\varphi(x)\wedge\varphi(y)=\varphi(x\wedge y)\in\varphi[L]$，故 $\varphi[L]$是 L 的子格。同理可以对 ψ 进行证明。

3. 共十个子群：A_4，$H_1=\{(1), (1\ \ 2)(3\ \ 4)\}$，$H_2=\{(1), (1\ \ 3)(2\ \ 4)\}$，$H_3=\{(1), (1\ \ 4)(2\ \ 3)\}$，$H_4$

$=\langle(1\ \ 2\ \ 3)\rangle$，$H_5=\langle(1\ \ 2\ \ 4)\rangle$，$H_6=\langle(1\ \ 3\ \ 4)\rangle$，$H_7=\langle(2\ \ 3\ \ 4)\rangle$，$B_4=\{(1),(1\ \ 2)(3\ \ 4),(1\ \ 3)(2\ \ 4),(1\ \ 4)(2\ \ 3)\}$，$H_0=\{(1)\}$. 其覆盖图如下．$\{H_0, H_4, A_4\}$和$\{H_0, H_1, B_4, A_4\}$都是覆盖链，但长度不同，由定理5，$A_4$的子群格不是模格.

4．B_4的子群覆盖图如418页所示．由于$H_1\wedge(H_2\vee H_3)=H_1\wedge B_4=H_1\neq H_0=H_0\vee H_0=(H_1\wedge H_2)\vee(H_1\wedge H_3)$，故$B_4$的子群格不是分配格.

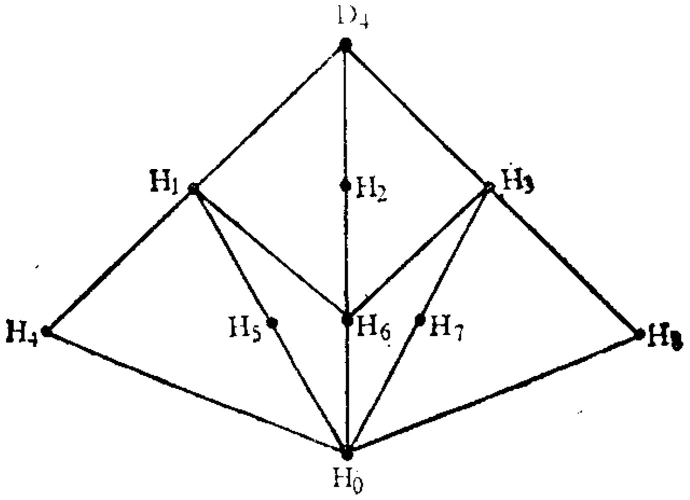


第4题图

5．设A，B，C是环R的理想，$B\leqslant A$，即$B\subseteq A$．$A\wedge(B\wedge C)=A\cap(B+C)$，$B\vee(A\cap C)=B+(A\cap C)$．任取$x\in A\cap(B+C)$，则$x\in A$，$x=b+c$，$b\in B$，$c\in C$，$c=x-b\in A$，因而$c\in A\cap C$，即$x\in B+(A\cap C)$．这证明$A\cap(B+C)\subseteq B+(A\cap C)$，或$A\wedge(B\vee C)\leqslant B\vee(A\wedge C)$．$(M_1)$成立.即环$R$的理想格是模格.

复习题七

1. 见习题3·6—2，依次编为 D_4, H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7, H_8(见此题答案)．其覆盖图如下．



第 1 题图

2. (1) 证 Σ 是半序集．任取 $R\in\Sigma$，显然 $R\leqslant R$（反身性）．如果 $R_1\leqslant R_2$, $R_2\leqslant R_1$，即当 aR_1b 时，有 aR_2b，而当 aR_2b 时，有 aR_1b，故 $aR_1b\Longleftrightarrow aR_2b$, $R_1=R_2$（反对称性）．如果 $R_1\leqslant R_2$, $R_2\leqslant R_3$，即对于 a, $b\in A$，由 aR_1b 推出 aR_2b，继而 aR_3b，因而 $R_1\leqslant R_3$（传递性）．(2) 证 Σ 与 $A\times A$ 子集半序集同构．设 S_R 是 $R\in\Sigma$ 对应的集合（见§1·4 二），于是 Σ 可与 $A\times A$ 子集族 $F(A\times A)$ 一一对应，这种对应是双向保序的，即 $R_1\leqslant R_2$ 等价于 $S_{R_1}\subseteq S_{R_2}$，所以两半序集同构．Σ 的单位元是全关系，零元是空关系．

3. 半序集的三条性质可由 L 的半序集性质逐一得到．如由 $f(x)\leqslant g(x)$, $g(x)\leqslant f(x)$，固定 x, $f(x)$, $g(x)\in L$，由 L 的反对称性，得 $f(x)=g(x)$, $x\in S$．如果 L 是格，规定 S 到 L 的映射 $l(x)$ 和 $m(x)$ 为：$l(x)=f(x)\vee g(x)$, $m(x)$

$=f(x)\wedge g(x)$，$x\in S$. 易证 $l(x)$是 $f(x)$，$g(x)$的上确界，$m(x)$是 $f(x)$与 $g(x)$下确界，因而 F 作成格.

4. 由 §7·2 定理 1 来证. $0\leqslant a$，故 $0\vee a=a$，$0\wedge a=0$. 又 $a\leqslant e$，故 $e\vee a=e$，$e\wedge a=a$. 若 $a\vee b=0$，则 $a=a\vee 0=a\vee(a\vee b)=(a\vee a)\vee b=a\vee b=0$，同理 $b=0$. 若 $a\wedge b=e$，则 $a=a\wedge e=a\wedge(a\wedge b)=(a\wedge a)\wedge b=a\wedge b=e$，同理 $b=e$.

5. 由格的定义，$\langle L,\vee\rangle$和$\langle L,\wedge\rangle$是群胚. 由 §7·2 定理 1 中(L_3)知是半群，由(L_2)知是可换半群. 格中单位元是$\langle L,\vee\rangle$的半群零元和$\langle L,\wedge\rangle$的半群单位元，格中零元是$\langle L,\vee\rangle$的半群单位元和$\langle L,\wedge\rangle$的半群零元.

6. 充分性：若 $b\leqslant a$，则 $a\wedge(b\vee c)=a\wedge((a\wedge b)\vee c)=(a\wedge b)\vee(a\wedge c)=b\vee(a\wedge c)$. 适合 §7·2($M$)式，故 L 为模格. 必要性：任取 a，b，$c\in L$，则 $a\wedge b\leqslant a$，由(M)，$a\wedge((a\wedge b)\vee c)=(a\wedge b)\vee(a\wedge c)$.

7. $a=a\vee(a\wedge c)=a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c)=(a\vee b)\wedge(b\vee c)=b\vee(a\wedge c)=b\vee(b\wedge c)=b$.

8. 设$\langle a\rangle$为 2^n 阶循环群，共 $n+1$ 个子群：$\langle a\rangle\supseteq\langle a^2\rangle\supseteq\cdots\supseteq\langle a^{2^{n-1}}\rangle\supseteq\langle a^{2^n}\rangle$，子群格系全序集，因而是分配格(§7·3 例 2).

9. 易见左式$\leqslant$右式，右式$\leqslant$左式.

10. 如果 c 覆盖 a 和 b，则 $a\vee b\leqslant c$. 如果 $c\neq a\vee b$，而因 $a\vee b$ 不会是 a 或 b，于是在 a 和 c 之间有中间元素 $a\vee b$，与 c 覆盖 a 矛盾，同样可证另一问题.

〔附录〕

本书符号表

$\mathbf{E}$	偶数集.
$\mathbf{D}$	奇数集.
$\mathbf{P}$	正整数集.
$\mathbf{N}$	非负整数集.
$\mathbf{Z}$	整数集.
$\mathbf{Z}^*$	非零整数集.
$\mathbf{Q}^+$	正有理数集.
$\mathbf{Q}^*$	非零有理数集.
$\mathbf{Q}$	有理数集.
$\mathbf{R}^+$	正实数集.
$\mathbf{R}^*$	非零实数集.
$\mathbf{R}$	实数集.
$\mathbf{C}^*$	非零复数集.
$\mathbf{C}$	复数集.
$\mathbf{Z}_n$	以 n 为模的剩余类.
$[a]$	包含 a 的类.
$A \sim B$	集合 A 与 B 等势.
$a \sim b$	a 与 b 等价.

aRb	a 与 b 有关系 R.
$a \in A$	a 属于 A.
$a \notin A$	a 不属于 A.
$A \subseteq B$	A 是 B 的子集.
$A \subset B$	A 是 B 的真子集.
$A \cup B$	A 与 B 的并.
$A \cap B$	A 与 B 的交.
$A \backslash B$	A 与 B 的差.
ϕ	空集.
$a \equiv b \pmod{n}$	a 与 b 模 n 同余.
$\lvert A \rvert$	集合 A 含元素个数.
$A \times B$	集合 A 与 B 积集.
A/E	集合 A 关于等价关系 E 的商集.
$\sigma[A]$	A 在映射 σ 下

	的象集。
$\sigma^{-1}[A]$	A 在映射 σ 下的原象集。
$F(A)$	集合 A 的子集族。
$M_n(R)$	环 R 上的 n 阶方阵集。
$M_n^*(R)$	实非退化 n 阶方阵集。
e_A	集合 A 的恒等变换。
$G(A)$	集合 A 的一一变换集。
$S(A)$	集合 A 的变换集。
$\langle A, \cdot \rangle$	群胚、半群或群。
$C(G)$	群 G 的中心。
$\langle a \rangle$	a 生成的循环群，或生成的理想。
$\langle S \rangle$	子集 S 生成的子群或理想。
$A(G)$	群 G 的自同构集。
$I(G)$	群 G 的全体内自同构集。
$E(G)$	群 G 的自同态集。
$G(A)$	半群 A 的可逆元集。
C_n	n 阶循环群。
C_∞	无限循环群。
U_n	n 次单位根集。
S_n	n 次对称群。
A_n	n 次交错群。
D_4	正方形对称群。
B_4	克莱茵四元群。
$N(a)$	a 的正规化子。
H	四元数代数。
O	凯莱代数。
$a \mid b$	a 整除 b。
$a \nmid b$	a 不整除 b。
a^{-1}	a 的逆元。
e	半群或群的单位元。
1	域的单位元。

0	零元。
$Hom(A,B)$	群 A 到群 B 的同态集合。
$\boldsymbol{R}_2$	平面向量集合。
$\boldsymbol{B}$	平面上的旋转变换集合。
$\boldsymbol{T}$	平面上的平移变换集合。
$F(x)$	域 F 上的分式域。
$F[x]$	域 F 上的多项式环。
$F^*[x]$	非零多项式集。
$F(a)$	a 生成的单扩域。
K_φ	同态 φ 的核。
$A\cong B$	A 同构于 B。
$\boldsymbol{Z}[i]$	高斯数环。
$\boldsymbol{Z}(i)$	高斯数域。
G/N	商群或商半群。
R/I	商环。
$\sqrt{P}$	理想 P 的根。
$\Leftrightarrow$	当且仅当，等价。
$\Rightarrow$	推出，则。
(a,b)	a 与 b 的最大公因子集；有时则表为有序对和开区间。
$(G:H)$	G 关于子群 H 的指数。
$[E:F]$	扩域 E 在 F 上的次数。
$(i\ \ j)$	对换。
$(i_1\ i_2\cdots i_k)$	循环。
R^*	环 R 的非零元集。
$\boldsymbol{R}_n$	实 n 维向量空间。
$F[0,1]$	区间 $[0,1]$ 上的实函数集。
$A(E\|K)$	域 E 的使子域 K 的元素不动的自同构集合。
$I(H)$	域中在 H 的元素作用下不

	动元集。
$\langle A,\leqslant\rangle$	半序集或全序集。
$\langle R,+,\cdot\rangle$	环。
$[a,b]$	李代数中 a,b 之积；有时则表闭区间；群中表示换位子；整数的最小公倍。
$a\vee b$	a 与 b 的上确界。
$a\wedge b$	a 与 b 的下确界。
A^-	结合代数 A 对应的李代数。
A^+	结合代数 A 对应的约当代数。

Document generated by Anna's Archive around 2023-2024 as part of the DuXiu collection
(https://annas-blog.org/duxiu-exclusive.html).

Images have been losslessly embedded. Information about the original file can be found in PDF attachments. Some stats (more in the PDF attachments):
{
"filename": "MTEwMjAzNThf5oq96LGh5Luj5pWwLnppcA==",
"filename_decoded": "11020358_\u62bd\u8c61\u4ee3\u6570.zip",
"filesize": 18000340,
"md5": "86d8ab0b092be0a5944d970cd4991e9b",
"header_md5": "cce5ab0441bdde7d22cdb644afa932d6",
"sha1": "c910f67abdf3546b05f214a58ea132d3c300175f",
"sha256": "e47151dee0908136b1e361e66306ebb8cc673e96f2a2a911a9a6525e941d87f4",
"crc32": 877639273,
"zip_password": "",
"uncompressed_size": 18972677,
"pdg_dir_name": "11020358_\u2502\u0398\u2567\u2264\u2524\u00b7\u2569\u00b2",
"pdg_main_pages_found": 426,
"pdg_main_pages_max": 426,
"total_pages": 437,
"total_pixels": 1442668544,
"pdf_generation_missing_pages": false
}